all rights reversed

HACKER

Season 05 / Issue 11

τεύχος 059 - Midday Launch Edition

Κυνήγι vulnerabilities & Linux desktops που πετάνε [*]

Nested virtualization για το KVM: γιατί και πώς

Το WannaCry του Linux και η εκμετάλλευσή του

Αυτοματοποιημένες εγκαταστάσεις με το AutoYaST

Αναβαθμίστε το Linux PC σας χωρίς να δώσετε ούτε ένα ευρώ

Εντοπίστε αδυναμίες σε συστήματα με το καινούργιο OpenVAS

Πώς κάνετε reset στο password του root, όταν δεν το γνωρίζετε

[*] γιατί καλοκαιρινή χαλάρωση δεν σημαίνει *μόνο* παραλία, ρακέτες και Despacito ;)

all rights reversed

HACKER


CMYK & WEB
cmykandweb.gr
GRAPHIC DESIGN
design • layout • web

#dH059 | Περιεχόμενα

Εκδότης / Διευθυντής	Χρήστος Βαρελάς
Αρχισυντάκτης	Παναγιώτης Βαρελάς
Σύμβουλοι έκδοσης	Βούλα Παυλίδου
Σύνταξη	Παναγιώτης Βαρελάς, Χρήστος Βαρελάς, Πάνος Γεωργιάδης, Γιώργος Γιάννου, Γιάννης Κρομμύδας, Πέτρος Κυλαδίτης, Μέσος Παπαδόπουλος (TM), Χρίστος Τόμπρας, @arkoudos
Γραμματική επιμέλεια	Βούλα Παυλίδου
Καλλιτεχνική Επιμέλεια	Πέτρος Φιλιππίδης

Το ψηφιακό περιοδικό deltaHacker είναι συνδρομητικό και εκδίδεται από την Parabing Creations. Ο δικτυακός τόπος του περιοδικού είναι στο https://deltahacker.gr και το email επικοινωνίας είναι το talk2us@deltahacker.gr. Οι γενικές πληροφορίες για τις συνδρομές παρατίθενται στο https://deltahacker.gr/order κι από την ίδια σελίδα γίνονται οι παραγγελίες.

Όχι πια ντοκ, μόνο εμ-ντι

του Χρήστου Βαρελά

Φίλες και φίλοι,

- Έχουν περάσει αρκετά χρόνια από την εποχή που χωρίς κανένα δισταγμό κατέφευγα στην "δεν έχω λεφτά για software" δικαιολογία, ώστε να τρέχω εμπορικό λογισμικό χωρίς να δίνω ούτε (μια δραχμή|ένα ευρώ).
- Είμαι πολύ καιρό σε ηλικία "μπορώ να πληρώνω για το software που χρειάζομαι", και καθόλου δεν χαλιέμαι. Όταν, π.χ., λίγα χρόνια πριν η Microsoft υιοθέτησε συνδρομητικό μοντέλο χρήσης για το Office, πρόθυμα επέλεξα να αποκτήσω κι εγώ τη συνδρομή μου. Το σκεπτικό ήταν ότι ήθελα να δουλεύω χωρίς τύψεις με τα Word κι Excel, ενώ δεν είχα καμία όρεξη να ψάχνω για σπασμένες εκδοχές που σήμερα παίζουν, αύριο δεν παίζουν. Όχι. Προτιμούσα να έχω το κεφάλι μου ήσυχο και να κάνω τη δουλειά μου όμορφα κι ωραία – ή έστω να προσπαθώ να την κάνω όμορφα κι ωραία.
- Είναι φυσικά και το άλλο: Από τη στιγμή που ο κατασκευαστής της σουίτας ζητά χρήματα –και μπράβο του–, γιατί εγώ να μην πληρώνω; Αν για οποιονδήποτε λόγο δεν θέλω ή δεν μπορώ, υπάρχουν ωραιότατες εναλλακτικές δωρεάν προτάσεις, όπως, π.χ., το LibreOffice (https://www.libreoffice.org). Αν δεν μου κάνει το LibreOffice (που παρεμπιπτόντως δεν μου κάνει και το αντιπαθώ έντονα), τότε ψάχνω για εναλλακτική δωρεάν λύση.
- Κάπως έτσι βλέπω τα πράγματα, φίλες και φίλοι.
- Μόνο που έναν περίπου μήνα πριν σταμάτησα και πάλι να πληρώνω για το Office.
- Δεν ανανέωσα την ετήσια συνδρομή μου, αλλά μη φανταστείτε ότι επέστρεψα στην παρανομία (υποχρεωτικά air quotes εδώ).
- Συχνά σκεφτόμουν ότι τα Word κι Excel είναι πολύ περισσότερο feature rich για τις ανάγκες μου. Είναι σαν να χρησιμοποιείς κανόνι για να πυροβολήσεις ένα σπουργίτι, όπως κάποτε είχε πει αγαπητός συνάδελφος σε άλλον, επίσης αγαπητό συνάδελφο. Αν και δεν ήμουν ποτέ φίλος του κυνηγιού, το νόημα της παρομοίωσης ήταν και παραμένει 110% ταιριαστό και για την περίπτωση που τώρα σας λέω.

- Αφού λοιπόν για τα κείμενα που έγραφα και τα λογιστικά φύλλα που συντηρούσα τα Word κι Excel ήταν (κι εξακολουθούν να είναι) overkill, γιατί μέχρι πρότινος τα χρησιμοποιούσα;
- Ίσως γιατί αμφότερες οι εφαρμογές δουλεύουν καλά, υπό την έννοια ότι δεν κρασάρουν σχεδόν ποτέ και ταυτόχρονα αποκρίνονται γρήγορα και προβλέψιμα. Επίσης, ένα άλλο θετικό με τη συνδρομή που πλήρωνα στη Microsoft, ήταν ότι διατηρούσα το δικαίωμα να εγκαθιστώ το Office σε PC, Mac, iOS κι Android. Σχεδόν πάντα συνηθίζω να δουλεύω σε τουλάχιστον δύο από τις τέσσερις αυτές πλατφόρμες, οπότε καταλαβαίνετε ότι η προσφερόμενη δυνατότητα δεν μπορούσε να περάσει απαρατήρητη.
- Την ίδια στιγμή διακατέχομαι κι από ισχυρές τάσεις μινιμαλισμού. Υπάρχουν μάλιστα περίοδοι κατά τις οποίες οι τάσεις αυτές θυμίζουν εμμονή. Πρόσφατη εκδήλωση κραυγαλέου μινιμαλισμού από μέρους μου, ήταν η υιοθέτηση του i3 window manager για τα συστήματα Linux που καθημερινά χρησιμοποιώ (https://deltahacker.gr/?p=17547). Πριν από τον i3, έβλεπα συναδέλφους να δουλεύουν με το tmuxκαι πωρωνόμουν (https://github.com/tmux/tmux/wiki). Παλιότερα, θυμάμαι ότι αδιαφορούσα για όλους τους torrent clients και χρησιμοποιούσα αποκλειστικά το rtorrent (https://github.com/rakshasa/rtorrent/wiki). Την περασμένη άνοιξη έπρεπε να στήσω ένα Ceph virtual cluster για εκπαιδευτικούς λόγους και testing. Ενώ για τη δημιουργία και τη διαχείριση εικονικών δικτύων και QEMU/KVM VMs κάλλιστα θα μπορούσα να καταφύγω στον Virtual Machine Manager, αποφάσισα και δούλεψα αποκλειστικά από τη γραμμή εντολών. (Εκτός από την ικανοποίηση του αισθήματος μινιμαλισμού, η απόφαση αυτή είχε κι άλλα οφέλη. Δεν είναι του παρόντος, οπότε δεν τα αναφέρω τώρα.)
- Στο ίδιο μήκος κύματος, λοιπόν, εδώ και λίγο καιρό σκεφτόμουν πώς θα καταφέρω να παραμερίσω τα Word κι Excel και βεβαίως με τι θα τα αντικαταστήσω. Τελικά το Excel το αντικατέστησα με το Numbers, το οποίο διατίθεται δωρεάν για τους υπολογιστές και τις συσκευές της Apple (https://www.apple.com/lae/numbers). Είναι απλό, γρήγορο, μπορεί να ανοίγει αρχεία του Excel, να κάνει export στα αντίστοιχα format, ενώ βεβαίως υποστηρίζει και το δικό του file format. Το θέμα με το Numbers είναι ότι τρέχει μόνο σε Mac OS X και iOS. Σε σχέση με το Excel, λοιπόν, τώρα πρέπει να λαμβάνω υπόψη την πλατφόρμα στην οποία βρίσκομαι και να σκέφτομαι δύο φορές πριν κάνω κάτι. Αλλά η κατάσταση δεν είναι τόσο τραγική. Όποτε έχω να κάνω επεμβάσεις σε κάποιο λογιστικό φύλλο και βρίσκομαι σε Linux ή σε Windows (σπάνιο), υπάρχει και το LibreOffice. Επίσης, τα λογιστικά φύλλα που κατά κύριο λόγο δουλεύω, συγγενεύουν περισσότερο με βάσεις δεδομένων παρά με spreadsheets. Ο παροπλι-

σμός του Excel, λοιπόν, θέλω να ελπίζω ότι θα με παρακινήσει στο να σχεδιάσω, επιτέλους, μια ή δύο βάσεις για τη MariaDB (https://mariadb.org). Βέβαια ακόμη κι αφού το κάνω, η ανάγκη για μερικά απλά spreadsheets θα παραμένει. Αλλά προσέξτε: μιλάμε για απλά spreadsheets, τα οποία οποιαδήποτε σχετική εφαρμογή μπορεί και τ' ανοίγει εύκολα.

- Και με το Word τι κάνουμε; Η αλήθεια είναι ότι το Word το χρησιμοποιώ περισσότερα χρόνια απ' όσα μπορώ να θυμηθώ. Κατά καιρούς είχα προσπαθήσει να το αντικαταστήσω με άλλες εφαρμογές – κι αυτή τη στιγμή στο νου έρχονται λέξεις όπως WordPerfect και StarWriter. Μετά όμως από κάθε απόκλιση ή έστω σκόπιμη εκστρατεία εξερεύνησης, πάντα στο Word γύριζα. Ανέκαθεν η εφαρμογή δούλευε καλά για 'μένα, ασχέτως της πολυπλοκότητας των κειμένων που είχα να προετοιμάσω. Η μόνη φορά που με θυμάμαι να βρίζω και να καταριέμαι το Word, ήταν όταν ένας καθηγητής, στο Πανεπιστήμιο, μου είχε ζητήσει να πληκτρολογήσω στο κομπιούτερ (έτσι τα λέγαμε τις Παλιές Καλές Μέρες™) ένα ολόκληρο βιβλίο Γραμμικής Άλγεβρας, κι άλλο ένα περί θεωρίας αυτομάτων, γλωσσών και γραμματικών (πάντα για Μαθηματικά μιλάμε). Είχα σκεφτεί ότι θα γράψω σε LaTeX (https://www.latex-project.org) και πολύ είχα χαρεί, όμως ο κος καθηγητής είχε άλλα σχέδια: τα βιβλία –αμφότερα δικά του, παρεμπιπτόντως–, ήθελε να τα έχει σε DOC format. Ξεκίνησα με όλη την καλή διάθεση, αναλογιζόμενος ότι μπροστά μου έχω μια πρώτης τάξεως ευκαιρία για να δοκιμάσω καλά τον αγαπημένο Equation Editor σε πραγματικές συνθήκες (https://en.wikipedia.org/wiki/Microsoft_Office_shared_tools#Equation_Editor). Πολύ γρήγορα συνειδητοποίησα ότι το PC μου χρειαζόταν τουλάχιστον τη διπλάσια RAM ώστε να ξεχάσει αυτή την εμμονή με το swapping, ενώ και μια ταχύτερη κάρτα γραφικών σίγουρα θα βοηθούσε σημαντικά. Περιττό να σημειώσω ότι δυνατότητα για αναβάθμιση δεν υπήρχε. Καταλαβαίνετε λοιπόν ότι αν το Υπέρτατο Ον, αυτό που αποφασίζει για το πού πάμε μετά, με πρόσεξε έστω και λίγο τον καιρό εκείνο, τώρα που μιλάμε έχω διασφαλισμένη τη θέση μου σε ένα άβολα ζεστό μέρος.
- Παιδεύτηκα λίγο με το ζήτημα της αντικατάστασης του Word, ώσπου ξαφνικά συνειδητοποίησα ότι η λύση είναι μπροστά στα μάτια μου (ή κάτω από τα δάκτυλά μου, μιας και μιλάμε για πληκτρολόγηση). Δεν αναφέρομαι σε κάποια εναλλακτική εφαρμογή, αλλά στη γλώσσα υποσημείωσης Markdown, την οποία εδώ κι αρκετό καιρό ούτως ή άλλως χρησιμοποιώ (https://deltahacker.gr/?p=10306). Χωρίς καλά καλά να το συνειδητοποιήσω η Markdown ήλθε κάποια στιγμή στην καθημερινότητά μου – κι απ' ό,τι όλα δείχνουν έχει έλθει για να μείνει. Το site του περιοδικού, για παράδειγμα, βασίζεται στο WordPress. Ένα από τα plugins που έχουμε μονίμως

ενεργοποιημένο είναι το Jetpack (https://jetpack.com). Στις δυνατότητες του Jetpack συμπεριλαμβάνεται η υποστήριξη της Markdown, ώστε από το back-end του WordPress να δημοσιεύεις απευθείας άρθρα γραμμένα στην εν λόγω γλώσσα. Για μήνες τώρα, έτσι δημοσιεύουμε στο site: γράφουμε απευθείας σε Markdown, ξεκινάμε νέο post στο WordPress κι αντιγράφουμε απευθείας τον "κώδικα" Markdown στο σχετικό πλαίσιο. Πρέπει να σημειώσω εδώ ότι τα παραγόμενα κείμενα, αυτά που βλέπουν οι επισκέπτες του deltaHacker, δείχνουν πολύ καθαρά κι όμορφα. Εντάξει, ίσως το theme στο site να ανήκει σε προηγούμενη δεκαετία, νομίζουμε όμως ότι τα κείμενα αυτά καθεαυτά είναι ευπαρουσίαστα κι άνετα στην ανάγνωση. Σε Markdown γράφω κι όταν, αραιά και που, αποφασίζω να δημοσιεύσω κάτι στο προσωπικό blog (https://colder.xyz). Χρησιμοποιώ επίσης Markdown και στην άλλη εργασία μου, για την παραγωγή documentation. (Προς το παρόν μόνο για προσωπική χρήση, κάτι μου λέει όμως ότι πολύ σύντομα θα ετοιμάζω documentation και για άλλους συναδέλφους. Πολλά περαστικά τους εύχομαι, από τώρα.)

- Η Markdown, λοιπόν, είναι ό,τι πρέπει για την περίπτωσή μου. Ένας καλός text editor με syntax highlighting μου έλειπε στην αρχή, αλλά πολύ γρήγορα (και με πολλή χαρά) κατέληξα στον Atom – σ' αυτόν γράφονται οι γραμμές τούτες! (https://atom.io) Ομολογώ ότι αρχικά είχα φλερτάρει με την ιδέα του vim, είπα όμως στον εαυτό μου ότι, εντάξει, καλές είναι αυτές οι ροπές προς τον μινιμαλισμό, δεν χρειάζεται όμως να τις ακολουθώ και με θρησκευτική ευλάβεια.

- Προς το παρόν, ο μόνος που έχει παραπονεθεί γι' αυτά τα αρχεία md είναι ο αγαπητός art director του περιοδικού. (Αυτά τα ωραία PDF των τευχών; (https://deltahacker.gr/?p=13867) Ε, δικά του πονήματα είναι!) Η αλήθεια είναι ότι τον βολεύει πολύ περισσότερο να του παραδίδουμε αρχεία DOC. Δεν είναι ότι δεν μπορεί ν' ανοίξει ή να κατανοήσει αρχεία md. Απλά, το InDesign CC που δουλεύει μπορεί και διαβάζει DOC, αλλά όχι md. Η προσωρινή λύση που εφαρμόζουμε δεν είναι η κομψότερη δυνατή, αλλά τουλάχιστον δουλεύει. Ας είναι καλά το Pages (https://www.apple.com/lae/pages) και η προθυμία κάποιων για λίγο manual work (ναι, στα αγγλικά, γιατί η "χειρωνακτική εργασία" ακούγεται κάπως).



σνέλ μέλ

Αγαπητοί μου,

Ήμασταν που λέτε το πρωί όλοι καθ' όλα έτοιμοι, με το κλειδί στο χέρι και όλα τα συμπράγκαλα: βαλίτσες, βαλιτσόπουλα, κουτιά, σακ-βουαγιάζ, ταπεράκια, σακούλες, βατραχοπέδιλα, αντηλιακό. Θα φεύγαμε για το σταθμό του ΚΤΕΛ αλλά κάτι έλειπε, το ένοιωθα, και δεν ήξερα τι.

Το κατάλαβα με το που κλειδώναμε την πόρτα. "Αμάν!", φώναξα, "η γραφομηχανή!"

"Μα τι την θέλεις την γραφομηχανή;" να ρωτάει εκνευρισμένη η μητέρα της εξαδέλφης, που είναι ινδουίστρια. "Τόσους μήνες την είχες να σκονίζεται. Τι σε έπιασε τώρα;"

Να σας πω την αλήθεια, πραγματικά δεν ξέρω κι εγώ τι με έπιασε. Κάποιο προαίσθημα, ίσως; Γιατί ---σύμπτωση άραγε;-- με το που μπαίνουμε στο λεωφορείο μου στέλνει φιρμάνι ο Κύριος Διευθυντής, πως καλό θα ήταν να του έχω ετοιμάσει την επιστολή πριν τελειώσει ο μήνας.

Έτσι λοιπόν, να 'μαστε στο Πόρτο Γερμενό, έτοιμοι να απολαύσουμε τις πρώτες στιγμές των φετινών μας διακοπών, κι εγώ στον βρεγμένο πάγκο με τη γραφομηχανή.

Ο πάγκος βρεγμένος γιατί προ ολίγου είχαμε μίαν ακόμα καλοκαιρινή νεροποντή, σαν αυτές που συνηθίζει φέτος τον Ιούλιο.

Λοιπόν, αυτό φέτος με τις νεροποντές μου θύμισε το καλοκαίρι του 2002. Δεν ξέρω αν το θυμάστε.

Κάθε πρωί χαρά Θεού. Ήλιος, τζιτζίκια, καύσωνας. Κάθε μεσημέρι, γύρω στις 3, ο ουρανός σκοτείνιαζε, μαζεύονταν από το πουθενά κάτι απίστευτα σύννεφα, κατράμι, και ξεκίναγε μια απίστευτη μπόρα. Κάθε μέρα. Για μισή ώρα, όχι παραπάνω. Κατά τις 4 ο ήλιος ήταν και πάλι ψηλά στον ουρανό. Σύννεφα πουθενά. Μόνο στους δρόμους και τα πεζοδρόμια έβλεπες τις ηγάδες με το νερό και θυμόσουν πως προ ολίγου μόλις γινότανε χαμός.

Το πράγμα συνεχίστηκε για εβδομάδες. Αν θυμάμαι καλά μας είχε πάει έτσι μέχρι τον Αύγουστο. Είχαμε όλοι σαστίσει. Είχα έναν φίλο ειδικά που το φαινόμενο τον είχε προβληματίσει πολύ.

"Δεν μπορεί να είναι τυχαίο", μου έλεγε. "Πώς μπορεί να είναι τυχαίο; Μα κάθε μεσημέρι; Την ίδια ώρα; Ραντεβού έχουν τα σύννεφα; Διαβασμένος άνθρωπος, δεν το βλέπεις πως δεν μπορεί να είναι τυχαίο;"

"Ε, και τότε τι;" του έλεγα εγώ. "Αν δεν είναι τυχαίο τι είναι;"

"Εμ, εδώ σε θέλω", ερχόταν η απάντηση. Αλλά δεν μου έλεγε. Ή δεν ήξερε ή δεν έλεγε.

Δύο χρόνια αργότερα, το καλοκαίρι του 2004, πάνω που ετοιμα-

ζόμουν να φύγω για να βρω τον ανιψιό στο Λονδίνο (και να αποφύγω τους Ολυμπιακούς), μου τα αποκάλυψε όλα.

Οι προγραμματισμένες βροχές του Ιουλίου 2002, ξεκίνησε να μου λέει, ήταν μέρος ενός σχεδίου των Αμερικάνων. Οι Αμερικάνοι διαθέτουν εδώ και δεκαετίες υψηλή τεχνολογία ελέγχου των μετεωρολογικών φαινομένων, αυτό είναι γνωστό. (Είναι; Εστω.) Οι συγκεκριμένες καταιγίδες ήταν προγραμματισμένες, ως μέρος της προσπάθειάς τους να εκφοβίσουν τις Ελληνικές Αρχές εν όψει των Ολυμπιακών Αγώνων. Οι Αμερικάνοι μας έδειχναν ποιος κάνει κουμάντο. Μας προειδοποιούσαν ότι, αν δεν συνεργαστούμε, έχουν την τεχνολογία να τα κάνουν όλα μαντάρα, από μετεωρολογικής πλευράς, και να οδηγήσουν τους Ολυμπιακούς σε αποτυχία.

Τον ευχαρίστησα που μοιράστηκε μαζί μου αυτή του την θεωρία και μπήκα γρήγορα γρήγορα στο αεροπλάνο.

Εφυγα για να πάω σε μια άλλη χώρα όπου οι καθημερινές βροχές τον Ιούλιο είναι συνηθισμένο φαινόμενο και δεν χρειάζεται να καταφύγεις σε, χμμ, τολμηρές ερμηνείες με μυστικές υπηρεσίες, βλοσυρούς επιστήμονες, σκοτεινά συμφέροντα και συγκεκαλυμμένες απειλές.

Καθισμένος νωρίτερα σήμερα στο λεωφορείο, έχοντας μόλις λάβει το φιρμάνι για την καινούργια επιστολή, και εντυπωσιασμένος από την σύμπτωση να έχω ψάξει να βρω τη γραφομηχανή πριν φύγουμε (σύμπτωση πράγματι;), αναλογιζόμουν για τους λόγους που μας κάνουν επιρρεπείς στους πλεκτανολογικούς μαιάνδρους.

Το θέμα έχει κάποιο ενδιαφέρον και θα άξιζε ο κόπος να το δούμε από λίγο πιο κοντά.

Λοιπόν, το φαινόμενο δεν μπορεί να εξηγηθεί αν δεν έχουμε πρώτα αναγνωρίσει ένα άλλο συνοδευτικό διανοητικό φαινόμενο, που μάλλον προηγείται. Θα το ονόμαζα fuzzy pattern recognition.

Πρόκειται για το φαινόμενο εκείνο που επιτρέπει στους μετεωρολόγους, ας πούμε, να ταξινομούν τα σύννεφα. Αν δεν ξέρεις από αυτά, όλα τα σύννεφα μοιάζουν ίδια. Λίγο πιο μαύρα, λίγο πιο άσπρα. Αλλά κατά βάση ίδια.

Όμως στην πραγματικότητα τα σύννεφα έχουν ξεκάθαρα ονόματα (θύσανοι, σωρείτες, στρώματα, σωρειτομελανίες κ.λπ. κ.λπ.), και οι μετεωρολόγοι έχουν λίγο πολύ σαφείς θεωρίες που εξηγούν και το γιατί λέγονται έτσι και το πώς έχουν σχηματιστεί.

Η γνώση αυτή δεν κατακτήθηκε από τη μία μέρα στην άλλη. Χρειάστηκαν δεκαετίες συζητήσεων κατά τον δέκατο ένατο αιώνα, προκειμένου να συμφωνήσουν οι ενδιαφερόμενοι για τα σημαντικά χαρακτηριστικά των σύννεφων και την ονοματολογία τους. Εδώ κολλάει αυτό που ονόμασα pattern recognition. Οι μετεωρολόγοι περιμένουν να δουν, και αναγνωρίζουν όταν βλέπουν, συγκεκριμένα pattern: θυσάνους, σωρείτες και λοιπά. Στην αρχή όμως συζητούσαν, και πολλές φορές διαφωνούσαν, για το ποιο ακριβώς είναι το pattern. Εξ ου και το fuzzy.

Fuzzy pattern recognition, λοιπόν.

Αλλά δεν θα αρκούσε αυτό. Για να επινοηθεί η μετεωρολογία χρειάζεται να έχει ήδη γίνει ένα ακόμα διανοητικό βήμα. Χρειάζεται να έχει γίνει αποδεκτή η ιδέα πως ο κόσμος και τα παρατηρούμενα σε αυτόν φαινόμενα υπακούουν σε κάποιο είδος λογικής.



Αυτή η ιδέα βρίσκεται στην καρδιά κάθε επιστημονικής δραστηριότητας. Για κάθε φαινόμενο ή αντικείμενο που η επιστήμη μελετά, υπάρχει η πεποίθηση πως κάπου υπάρχει κάποια εξήγηση, ισχύει κάποιος νόμος. Γι' αυτό και τα μελετάμε άλλωστε. Αν πραγματικά πιστεύαμε ότι το τάδε ή το δείνα φαινόμενο είναι απολύτως τυχαίο, δεν θα τα μελετούσαμε καθόλου. Δεν θα άξιζε ο κόπος.

Αυτό ισχύει ακόμα και για τα χαοτικά φαινόμενα. Και εδώ η πεποίθηση είναι πως, πίσω από το εμφανές χάος, υφίσταται κάποια λογική.

Η επιστημονική έρευνα, λοιπόν, ξεκινάει από την πεποίθηση (αξίωμα) πως ο κόσμος είναι ερμηνεύσιμος, συνεχίζει με fuzzy pattern recognition, και καταλήγει στον προσδιορισμό των σημαντικών μεγεθών και παραμέτρων του εκάστοτε φαινομένου, των σχέσεών τους και των νόμων που διέπουν αυτές τις σχέσεις. Καρπός της επιστημονικής έρευνας είναι ένα κατά το δυνατόν αντιπροσωπευτικό μαθηματικό μοντέλο του υπό μελέτη φαινομένου.

Οι ιουλιάτικες καταιγίδες του 2002 δεν αποτελούσαν αίνιγμα για τους μετεωρολόγους. Η ερμηνεία ήταν απλή και είχε κάτι να κάνει με τις μετακινήσεις αέριων μαζών από το βορρά, τις προϋπάρχουσες (και αναμενόμενες για την εποχή) υψηλές θερμοκρασίες στην Ελλάδα, τους αντικυκλώνες λόγω της διαμόρφωσης του εδάφους κ.λπ. κ.λπ.

Ο φίλος μου όμως αδιαφορούσε για όλα αυτά. Δεν του αρκούσε η μετεωρολογική εξήγηση του φαινομένου. Έψαχνε να βρει την κρυφή πρόθεση. Έψαχνε να αποκαλύψει την πλεκτάνη.

Πώς μπορούμε να το καταλάβουμε αυτό;

Αυτή η ιδέα, πως ο κόσμος υπακούει σε κάποιο είδος λογικής, η οποία μπορεί να περιγραφεί με την βοήθεια μεγεθών, παραμέτρων, νόμων κ.λπ., δεν είναι τόσο αυτονόητη όσο φαίνεται. Βασίζεται με την σειρά της σε μιαν ακόμα παραδοχή: πως τα μεγέθη και οι παράμετροι του κόσμου αυτού μπορούν να μετρηθούν --να αντιστοιχηθούν, δηλαδή-- σε αριθμούς ή σε σειρές αριθμών σε κάποια κλίμακα. Χωρίς αυτή την δεύτερη παραδοχή, οι επιστημονικοί νόμοι όπως, για παράδειγμα, ο νόμος της επιτάχυνσης (F = m x γ) ή οι εξισώσεις του Einstein (E = m x c^2), θα ήταν κενοί περιεχομένου.

Πρόκειται για μία από τις δύο σημαντικότερες διαφορές μεταξύ της νεωτερικής επιστήμης (της επιστήμης από τον Γαλιλαίο και μετά) και της επιστήμης των αρχαίων Ελλήνων. Οι αρχαίοι ημών δεν ενδιαφέρονταν για τη μέτρηση των μεγεθών, αλλά για την σύγκριση και το ποιόν τους. Δεν τους ενδιέφερε το "πόσο". Τους ενδιέφερε το περί τίνος πρόκειται. Το αν είναι μεγαλύτερο ή πιο μικρό. Το αν είναι βαρύτερο ή πιο ελαφρύ.

Παράδειγμα; Η γεωμετρία. Τα εργαλεία του γεωμέτρη ήταν ο χάρακας και ο διαβήτης, όχι το μοιρογνωμόνιο ούτε το υποδεκάμετρο. Το εργαλείο του μηχανικού ήταν ο ζυγός. Δεν σου έλεγε ποιο είναι το βάρος κάποιου πράγματος. Σου έλεγε ποιο από δύο πράγματα είναι βαρύτερο.

Αυτή είναι η μία διαφορά.

Η δεύτερη θεμελιώδης διαφορά της αρχαίας επιστήμης από τη νεωτερική είχε να κάνει με την αντίληψή της για τον ίδιο τον κόσμο. Κατά τους αρχαίους ο κόσμος δεν ήταν ενιαίος. Άλλα πράγματα ίσχυαν ψηλά στον ουρανό, και άλλα πάνω στην Γη. Ο κόσμος των ουράνιων σωμάτων ήταν κατά τους αρχαίους άπειρος, αρμονικός, αέναος, αμετάβλητος. Ο επίγειος κόσμος από την άλλη ήταν προσωρινός, ατελής, πεπερασμένος, μεταβαλλόμενος.

Για τους αρχαίους, όλες οι μεταβολές στον επίγειο κόσμο (σαφής απόδειξη της ατέλειάς του) γίνονται επειδή κάτι τις προκαλεί. Υπάρχουν αιτίες και υπάρχουν αποτελέσματα. Οι μεταβολές διαρκούν επί όσο χρειάζεται μέχρι να επιτευχθεί ξανά η ισορροπία που διαταράχτηκε από τον άλφα ή το βήτα λόγο. Η πέτρα, για παράδειγμα, θα κατρακυλήσει επειδή την κλώτσησες, αλλά αμέσως θα βρει κάπου να ηρεμήσει. Θα μείνει εκεί μέχρι να την κουνήσει κάτι άλλο. Αν δεν την

κουνήσει δεν θα κουνηθεί. Πίσω από κάθε μεταβολή υπάρχει μια πρόθεση.

Στον ουρανό, από την άλλη, δεν υπάρχουν μεταβολές. Τα αστέρια, ο ήλιος, το φεγγάρι, κινούνται με αιώνια περιοδικότητα στις τέλειές τους τροχιές. Οι πλανήτες περιφέρονται ανάμεσά τους κατά συγκεκριμένους τρόπους. Κοιτάς τον ουρανό και είναι πάντα ο ίδιος. Ο ουράνιος κόσμος δεν μεταβάλλεται, δεν κρύβει εκπλήξεις, είναι τέλειος.

Ο κόσμος στα μάτια της αρχαίας επιστήμης ήταν πολύ διαφορετικός από τον κόσμο στα μάτια του Γαλιλαίου και της νεωτερικής επιστήμης. Η αρχαία επιστήμη ήταν απολύτως και θεμελιωδώς ασύμβατη με την νεωτερική. Καμία από τις δύο δεν ήταν καλύτερη ή χειρότερη. Είναι διαφορετικές. Μιλάνε για διαφορετικά θέματα, θέτουν διαφορετικές ερωτήσεις, και ψάχνουν για διαφορετικού τύπου απαντήσεις.

Μεταξύ της αρχαίας και της νεωτερικής επιστήμης υπήρξε ρήξη, ρήξη την οποία προκάλεσε άθελά του ο Γαλιλαίος στην προσπάθειά του να απαγκιστρωθεί από τους περιορισμούς του Καθολικού Δόγματος. Βλέπετε, η αρχαιοελληνική διάκριση μεταξύ επίγειου και ουράνιου κόσμου βόλευε μια χαρά την Εκκλησία: ο ουράνιος κόσμος, ο κόσμος του Θεού και των αγγέλων, διατηρούσε την τελειότητά του, ενώ ο επίγειος, ένας κόσμος ατελής και περιορισμένος, εξηγούσε και τη ροπή του ανθρώπου προς την αμαρτία αλλά και την αναγκαιότητα για την τελική κρίση. Ο Γαλιλαίος όμως ήθελε τη Γη να υπακούει στους ίδιους νόμους με αυτούς που υπάκουαν και τα ουράνια σώματα. Εξ ου και το "Και όμως, κινείται" που θα έχετε ακούσει, δεν μπορεί.

(Γκουγκλ.)

Ας σχολιάσω, παρεμπιπτόντως, πως η επιστήμη δεν προχώρησε ποτέ πάνω σε μιαν ευθεία ολοένα και πληρέστερης γνώσης, ενώ και το τελικό διακύβευμα της επιστημονικής έρευνας δεν ήταν ποτέ η αλήθεια ως αλήθεια -- whatever that means. Αυτό καλό είναι να το θυμόμαστε όποτε μας ζαλίζουν τα αφτιά για την επιστημονική πρόοδο και για τα επιτεύγματα της τεχνολογίας. Θα μου επιτρέψετε, ωστόσο, αγαπητοί μου, να μην επεκταθώ. Next time.

Ξεκίνησα να μιλάω για τους πλεκτανολόγους, και κατέληξα να μιλάω για την επιστημονική μέθοδο και για τις διαφορές αρχαίας από νεωτερική επιστήμη. Δεν ήταν τυχαίο (!). Το αντίθετο μάλιστα.

Η βασική ιδέα κάθε πλεκτανολογικής προσέγγισης είναι ακριβώς αυτό, πως τα πράγματα "δεν είναι τυχαία". Όπως ακριβώς ο επιστήμονας έτσι και ο πλεκτανολόγος, σκύβουν πάνω από τα φαινόμενα και προσπαθούν, με τη βοήθεια της μεθόδου που περιέγραψα ως fuzzy pattern recognition, να κάνουν δύο πράγματα: να προσδιορίσουν τα σημαντικά μεγέθη και τις παραμέτρους του φαινομένου, και να διακρίνουν τις σχέσεις με τις οποίες συνδέονται.

Αντίθετα από τους επιστήμονες, ωστόσο, που αρκούνται στην πεποίθηση πως ο κόσμος υπακούει σε κάποια λογική και επιζητούν να διατυπώσουν τους νόμους αυτής της λογικής, κάποιοι άλλοι, εκείνοι που τώρα περιγράφω ως πλεκτανολόγους, θεωρούν πως τα φαινόμενα του κόσμου τούτου ενέχουν ένα "διότι" ή ένα "προκειμένου να" -- δηλαδή μια πρόθεση.

Όπως ο φίλος για τον οποίο σας έλεγα. Δεν του αρκούσε η μετεωρολογική ερμηνεία των καθημερινών εκείνων καταιγίδων το καλοκαίρι του 2002. Έψαχνε να βρει ποιος τις σχεδίασε και ποιόν ωφελούν.

Θα μπορούσε κανείς να πει πως οι πλεκτανολόγοι, εν αγνοία τους, βρίσκονται με το ένα πόδι στην νεωτερική και με το άλλο στην αρχαία επιστήμη. Δεν τους αρκεί η επιστημονική περιγραφή. Ψάχνουν να βρουν και την πρόθεση.

Ίσως εκεί να έγκειται το ζήτημα.

Ίσως σε όλους μάς αρέσει να φανταζόμαστε πως για ό,τι συμβαίνει υπάρχει πρόθεση.

Ίσως μας καθησυχάζει αυτό, και κάνει τη ζωή μας να μοιάζει λιγότερο τυχαία.

Αλλά ας το αφήσω και αυτό για την άλλη φορά.

Σας ασπάζομαι,
Θείος Ακάκιος

Skill: Intermediate
Tags: i3wm, Linux, openSUSE, Window Managers

i3wm: Σημαντική αναβάθμιση του συστήματός σας, δωρεάν!

Στην αγαπημένη σας διανομή Linux ο window manager είναι το λογισμικό που ελέγχει την τοποθέτηση και την εμφάνιση των παραθύρων στην οθόνη, στο πλαίσιο του χρησιμοποιούμενου περιβάλλοντος γραφικών. Ο window manager παίζει σημαντικό ρόλο σε αυτό που ονομάζουμε "εμπειρία χρήσης" και σε γενικές γραμμές κάνει τη ζωή μας ευκολότερη.

Υπάρχουν όμως και περιπτώσεις που μας εμποδίζει από το να είμαστε 100% παραγωγικοί. Την ίδια στιγμή καταναλώνει πολύτιμους πόρους συστήματος, χωρίς εμείς να αποκομίζουμε κάποιο ουσιαστικό όφελος.

Στο παρόν άρθρο παρουσιάζουμε και γνωρίζουμε τον i3 window manager (https://i3wm.org), εν συντομία i3wm ή απλά i3, ο οποίος απευθύνεται σε χρήστες που θέλουν να εστιάζουν στην εκάστοτε εργασία και να μην απασχολούνται από τις ιδιαιτερότητες του περιβάλλοντος γραφικών. Κατά νου έχουμε developers, διαχειριστές δικτύων, φοιτητές και σπουδαστές που δουλεύουν στις διπλωματικές ή στα διδακτορικά τους, ερευνητές ασφαλείας, επιστήμονες, QA engineers κ.ά.

Στα δυνατά σημεία του i3wm συγκαταλέγονται οι χαμηλές του απαιτήσεις σε πόρους συστήματος: αφού εγκαταστήσετε τον i3 κι αρχίσετε να εργαζόσαστε στο σπαρτιάτικο περιβάλλον του, σχεδόν αμέσως θα αισθανθείτε σαν να αποκτήσατε καινούργιο, γρηγορότερο υπολογιστή. Προκειμένου να σχηματίσουμε μια πρώτη εικόνα για τον i3wm, αξίζει να δούμε τέσσερις μεγάλες κατηγορίες window managers.

Compositing. Τα παράθυρα δημιουργούνται και σχεδιάζονται σε ξεχωριστά buffers. Ο window manager συνθέτει (composes) τα buffers δημιουργώντας μια εικόνα που αναπαριστά ό,τι προβλέπεται να βλέπουμε στην οθόνη, μετά γράφει τα αποτελέσματα στη display memory. Οι λεγόμενοι compositing window managers συνήθως επεξεργάζονται περαιτέρω τα παράθυρα στα buffers, εφαρμόζοντας εφέ 2D/3D και animations όπως blurring, fading, scaling κ.ο.κ. Παρουσία του κατάλληλου hardware και βεβαίως των αντίστοιχων drivers, εφέ όπως σκιές, live previews και animations

εκτελούνται ομαλά και σε πραγματικό χρόνο. Παραδείγματα compositing window managers αποτελούν ο Quartz Compositor στο Mac OS X, τα Compiz, KWin και Mutter για διάφορα περιβάλλοντα γραφικών στο Linux, καθώς κι ο Desktop Window Manager στα Microsoft Windows.

Stacking. Ονομάζονται και floating window managers και σχεδιάζουν όλα τα παράθυρα σε μια συγκεκριμένη σειρά με βάση τον painter's algorithm (https://en.wikipedia.org/wiki/Painter%27s_algorithm), επιτρέποντας τους να αλληλοκαλύπτονται. Όλοι οι window managers που επιτρέπουν την αλληλοκάλυψη παραθύρων χωρίς να είναι compositors, εμπίπτουν στη συγκεκριμένη κατηγορία. Τα παράθυρα σχεδιάζονται ένα ένα και η διαδικασία ξεκινά με το ίδιο το desktop, μετά με το παράθυρο ή τα παράθυρα που είναι πιο κοντά στο desktop (άρα πιο μακριά σε σχέση με τον χρήστη) κ.ο.κ. Φυσικά, ο σχεδιασμός ενός παραθύρου επιτρέπεται ακόμη κι αν καλύπτει εν μέρει (ή και ολικά) παράθυρα που έχουν ήδη σχεδιαστεί. Τα Windows 1.0 καθώς και το Classic Mac OS χρησιμοποιούσαν stacking window managers. Οι δε awesome (με πεζό "a") και Window Maker αποτελούν άλλα δύο παραδείγματα stacking window managers που συναντάμε στις διανομές του Linux.

Tiling. Σε αντίθεση με τους floating, οι tiling window managers χωρίζουν την οθόνη σε μη-αλληλοκαλυπτόμενα πλαίσια. Κάθε πλαίσιο είναι δυνατόν να περιλαμβάνει ένα παράθυρο ή δύο, επίσης μη-αλληλοκαλυπτόμενα πλαίσια. Ο i3 εξ ορισμού συμπεριφέρεται ως ένας tiling window manager, έχει όμως τη δυνατότητα να συμπεριφέρεται κι ως floating. Ακριβώς γι' αυτό το λόγο ανήκει στην κατηγορία των dynamic window managers.

Dynamic. Οι window managers της κατηγορίας μπορούν και συμπεριφέρονται είτε ως stacking (floating) είτε ως tiling. Όπως αναφέραμε μόλις, ο i3wm είναι ένας τέτοιος window manager. Άλλοι εκπρόσωποι της κατηγορίας είναι οι awesome, xmonad κι ο θρυλικός FVWM.

Για το υπόλοιπο του άρθρου στρέφουμε την προσοχή μας στον i3wm. Εννοείται ότι μας ενδιαφέρει να τον εγκαταστήσουμε, να τον φέρουμε στα μέτρα μας και να αρχίσουμε να εργαζόμαστε στο περιβάλλον του. Υποψιαζόμαστε ότι είτε θα τον λατρέψετε, είτε θα αδιαφορήσετε παντελώς για την ύπαρξή του. Προσέξτε: Σε καμία περίπτωση δεν λέμε ότι θα τον μισήσετε – αλλά μπορεί και να κάνουμε λάθος :P Ας αφήσουμε όμως τη συζήτηση κι ας περάσουμε στη δράση.

Εγκατάσταση και βασική ρύθμιση

Δουλεύουμε σε ένα σύστημα με openSUSE Leap 42.2 και περιβάλλον γραφικών το GNOME. Αυτό το τελευταίο βέβαια δεν έχει κάποια σημασία για τον i3: στις εγκαταστάσεις Linux συχνά συνυπάρχουν περισσότερα από ένα περιβάλλοντα γραφικών και, κατά το login στο λογαριασμό ενός χρήστη, είτε ενεργοποιείται το προκαθορισμένο περιβάλλον είτε επιλέγεται ένα από τα υπόλοιπα που είναι παρόντα στο σύστημα.

Πρώτο μας μέλημα τώρα είναι να εγκαταστήσουμε τον i3 window manager, μαζί με μερικά χρήσιμα εργαλεία. Με δικαιώματα διαχειριστή, σε ένα τερματικό πληκτρολογούμε `zypper ref` ώστε να επικαιροποιήσουμε τα repositories της διανομής. Μετά εφαρμόζουμε τα όποια διαθέσιμα patches γράφοντας `zypper patch` κι ακολούθως έρχεται η σειρά του i3 κι ορισμένων καλών φίλων:

```
zypper -n in i3 i3status i3lock dmenu feh
```

Ας δούμε λίγο καθένα από τα πέντε αυτά RPM packages.

i3: το πακέτο του i3, του dynamic window manager που μόλις εγκαταστήσαμε στο openSUSE μας

i3status: utility που παράγει strings με πληροφορίες για την i3bar, την προκαθορισμένη μπάρα του i3

i3lock: όταν ενεργοποιείται κλειδώνει την οθόνη κι επιτρέπει την πρόσβαση μόνον αφού πληκτρολογηθεί σωστά το password του χρήστη

dmenu: utility για τη γρήγορη εκκίνηση εφαρμογών

feh: ευέλικτος image viewer, χρησιμεύει και για τον καθορισμό wallpaper

Αυτή τη στιγμή ο i3 πρέπει να είναι εγκατεστημένος και μπορούμε να κάνουμε logout από το τρέχον GNOME session. Κατά τα αναμενόμενα, θα εμφανιστεί η οθόνη login του GDM – ή όποιου άλλου login manager χρησιμοποιείτε, τέλος πάντων. Πριν συνδεθούμε στο λογαριασμό του χρήστη μας, πατάμε στο εικονίδιο με το γρανάζι κι επιλέγουμε τον i3.

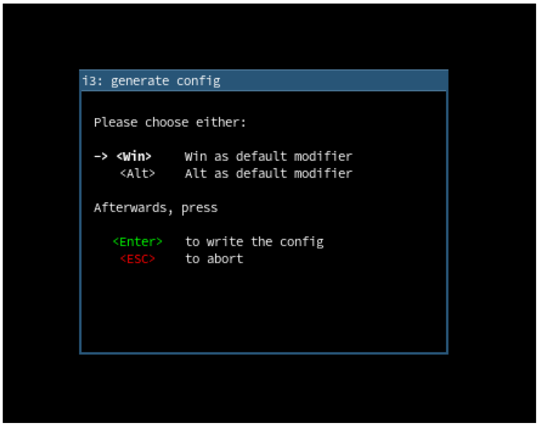


Επιλογή του i3 window manager, λίγο πριν συνδεθούμε στο λογαριασμό του χρήστη User Userson.

Την πρώτη φορά που θα ενεργοποιηθεί ο i3 για το λογαριασμό του χρήστη μας, βλέπουμε μια σχεδόν άδεια οθόνη κι ένα λιτό παράθυρο για τη βασική ρύθμιση του window manager. Το font rendering μάλλον δεν θα σας ικανοποιήσει, αλλά μην ανησυχείτε: μπορούμε να ορίσουμε οικογένεια γραμματοσειράς – και λίγο αργότερα θα δείξουμε πώς. Στην ερώτηση περί αυτόματης δημιουργίας του σχετικού αρχείου ρυθμίσεων απαντάμε καταφατικά, που σημαίνει ότι απλά πιέζουμε το πλήκτρο [Enter].



Την πρώτη φορά που θα φορτωθεί ο i3wm για τον χρήστη μας, είναι καλή ιδέα να δώσουμε το ΟΚ για την αυτόματη δημιουργία ενός βασικού αρχείου ρυθμίσεων.



Δεν ξέρουμε πώς το βλέπετε εσείς, εμείς όμως ησυχάζουμε και γαληνεύουμε όταν το modifier key είναι αντιστοιχισμένο στο πλήκτρο Windows (ή στο πλήκτρο Command).

Η δεύτερη και τελευταία ερώτηση που μας απευθύνεται σχετικά με τη δημιουργία του configuration file, αφορά στο modifier key ($mod key). Το εν λόγω πλήκτρο έχει εξαιρετική σημασία στον κόσμο του i3, αφού συμμετέχει στο σχηματισμό των key bindings για το χειρισμό του περιβάλλοντος και τη μετακίνησή μας μέσα σε αυτό. Τώρα, λοιπόν, καλούμαστε να αντιστοιχίσουμε το $mod key είτε στο πλήκτρο [Alt] είτε στο πλήκτρο [Win] (ή στο [Command], αν μιλάμε για Apple keyboard). Εξ ορισμού το $mod key είναι αντιστοιχισμένο στο [Win]/[Command]. Προσωπικά μάς αρέσει αυτό, οπότε απλά πατάμε το [Enter] και χωρίς άλλη καθυστέρηση το configuration του i3 δημιουργείται.

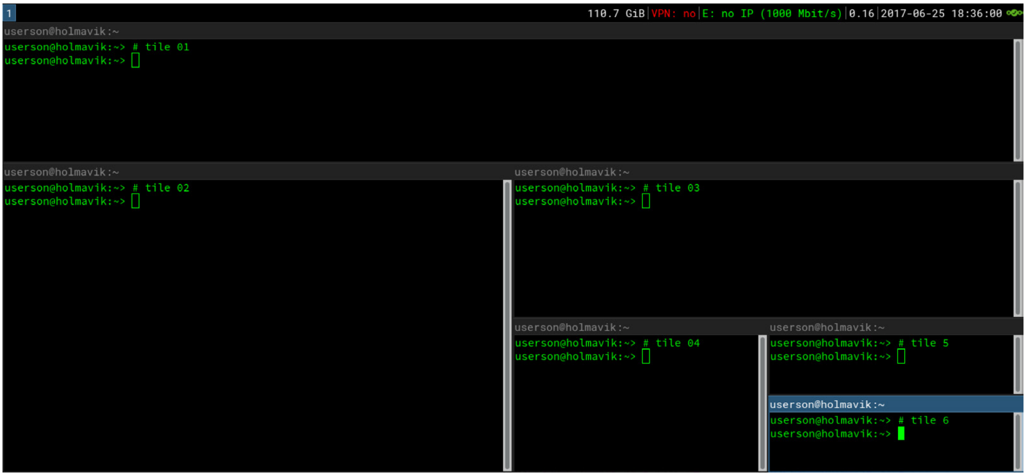
Πού βρισκόμαστε και τι κάνουμε

Πρόκειται βεβαίως για διαχρονικό υπαρξιακό ερώτημα, καταδικασμένο να μη λάβει ποτέ 100% ικανοποιητική απάντηση. Εκτός κι αν μιλάμε για τον κόσμο του i3 και μόνον αυτόν, οπότε σε αυτή την περίπτωση όλο και κάποια χρήσιμη απάντηση μπορούμε να δώσουμε.

Το μυστικό για καλή ζωή στον i3 είναι τα key bindings. Όσο πιο γρήγορα μάθουμε κάποια από αυτά, τόσο πιο γρήγορα θα εκτιμήσουμε τον window manager – ή θα αποφασίσουμε ότι δεν είναι για εμάς. Στο επίσημο site του i3 υπάρχει μια χρήσιμη σελίδα με key bindings (https://i3wm.org/docs/refcard.html). Προτείνουμε να δημιουργήσετε ένα σχετικό bookmark ή ακόμη και να την εκτυπώσετε.

Προς το παρόν, σημειώστε ότι για το άνοιγμα ενός terminal απλά πατάμε το συνδυασμό πλήκτρων [$mod + Enter] κι ακαριαία εμφανίζεται ένα μεγιστοποιημένο παράθυρο τερματικού. Αν δώσουμε άλλο ένα [$mod + Enter], η οθόνη τότε χωρίζεται στα δύο κι έχουμε δύο τερματικά. Παρατηρήστε ότι ο χωρισμός γίνεται κάθετα ή οριζόντια, αναλόγως αν ο προσανατολισμός της οθόνης είναι οριζόντιος (wide display) ή κάθετος (rotated display) αντίστοιχα. Για τη συνέχεια υποθέτουμε ότι δουλεύουμε με μία μόνο οθόνη, η οποία είναι προσανατολισμένη οριζόντια (δεν είναι rotated, δηλαδή). Δοκιμάστε να ανοίξετε κι άλλα παράθυρα τερματικού και δείτε πώς διευθετούνται. Αν θέλουμε το παράθυρο με το focus να είναι σε full screen mode, πατάμε το συνδυασμό [$mod + F]. Για να το επαναφέρουμε, πατάμε ξανά [$mod + F]. Κλείστε ένα οποιοδήποτε τερματικό που έχει το focus πατώντας, κατά τα γνωστά, [Ctrl + D] ή γράφοντας `exit`, ακολουθούμενο από [Enter]. Γενικά, μια οποιαδήποτε εφαρμογή στον i3 την κλείνουμε με το συνδυασμό πλήκτρων [$mod + Shift + Q]. Προτείνεται πάντως να χρησιμοποιούμε το μηχανισμό εξόδου/τερματισμού που προσφέρει η ίδια η εφαρμογή.

Αφήνουμε τώρα στην οθόνη μόνο ένα τερματικό ανοικτό. Η επόμενη κίνησή μας θα είναι να τρέξουμε τον Firefox. Όμως πριν το κάνουμε πατάμε [$mod + V]. Αυτή η ενέργεια δεν φαίνεται να έχει κάποιο αποτέλεσμα. Στην πραγματικότητα, όμως, μόλις είπαμε στον i3 ότι πλέον θέλουμε τα παράθυρα να χωρίζονται οριζόντια (κι όχι κάθετα). Δίνουμε [$mod + D], ώστε να ενεργοποιηθεί το dmenu. Παρατηρήστε την οριζόντια μπάρα, στο πάνω μέρος της οθόνης. Στη θυρίδα πάνω αριστερά, γράφουμε το όνομα του εκτελέσιμου μιας οποιασδήποτε εφαρμογής με GUI και πατάμε [Enter]. Δίνοντας, λοιπόν, [$mod + D] και πληκτρολογώντας `firefox` (ακολουθούμενο από [Enter]), ο Firefox ανοίγει. Διαπιστώνουμε ότι η οθόνη έχει χωριστεί σε δύο μέρη, οριζόντια: στο πάνω μέρος έχουμε το τερματικό, στο κάτω έχουμε τον Firefox. Με το focus στον Firefox, πατάμε [$mod + H]. Και πάλι δεν φαίνεται να συμβαίνει κάτι, στοιχηματίζουμε όμως ότι μαντεύετε τι έχει γίνει, καθώς και τι θα ακολουθήσει. Με [$mod + D] εμφανίζουμε το dmenu, ώστε να τρέξουμε άλλη μια εφαρμογή. Αυτή τη φορά πληκτρολογούμε `gnome-terminal` και φυσικά πατάμε το [Enter]. Αμέσως θα εμφανιστεί ένα παράθυρο του GNOME Terminal αλλά στο κάτω μισό της οθόνης και συγκεκριμένα στο δεξί μισό του κάτω μισού, δίπλα από τον Firefox. Προφανώς, λοιπόν, με [$mod + V] ορίζουμε ότι ο χωρισμός των παραθύρων γίνεται οριζόντια, ενώ με [$mod + H] ορίζουμε ότι ο χωρισμός των παραθύρων γίνεται κάθετα. Δοκιμάστε να ανοίξετε διάφορα παράθυρα χωρίζοντας οριζόντια ή κάθετα. Αν θέλετε, ανοίγετε το ίδιο παράθυρο αλλάζοντας διαδοχικά τη διεύθυνση του χωρισμού, ώστε τελικά να πάρετε στην οθόνη κάτι που θα μοιάζει με fractal. Από ένα σημείο και μετά αρχίστε να δίνετε τυχαία το focus σε παράθυρα (απλά μετακινείτε τυχαία τον δείκτη του ποντικιού) και κλείνετέ τα. Παρατηρήστε πώς ανταποκρίνεται ο i3, τακτοποιώντας αυτόματα τα εναπομείναντα ανοικτά παράθυρα.



Δεν έχει κάποια πρακτική σημασία η συγκεκριμένη διευθέτηση των παραθύρων, εκτός ίσως από το να δείξουμε πώς τοποθετεί τα tiles ο i3 όταν αλλάζουμε διαδοχικά τη διεύθυνση χωρισμού (οριζόντια, κάθετη). Αλήθεια, πόσο αναλυτικό μπορεί να γίνει το εικονιζόμενο fractal στη δική σας οθόνη;

Αναφερθήκαμε μόλις στην αλλαγή focus, με τη μετακίνηση του δείκτη του ποντικιού. Ο i3 όμως δίνει έμφαση στη χρήση του πληκτρολογίου και συνεπώς υπάρχουν ήδη key bindings για την αλλαγή του focus. Συγκεκριμένα, με [$mod + J] το focus πηγαίνει στο παράθυρο αριστερά, με [$mod + ;] στο παράθυρο δεξιά, με [$mod + L] πάνω, ενώ με [$mod + K] κάτω. Αν αντί για [$mod] + [J]/[;]/[L]/[K] πατήσουμε [$mod + Shift] + [J]/[;]/[L]/[K], το τρέχον παράθυρο μετακινείται αριστερά/δεξιά/πάνω/κάτω αντίστοιχα. Επίσης, αντί για τα πλήκτρα [J], [;], [L] και [K], μπορούμε να χρησιμοποιούμε τα αντίστοιχα βελάκια του δρομέα.

Ας υποθέσουμε τώρα ότι θέλουμε να αλλάξουμε το μέγεθος ενός παραθύρου. Αρχικά δίνουμε [$mod + R] και μετά παίζουμε με τα βελάκια. Θα δούμε το μέγεθος του επιλεγμένου παραθύρου να μεταβάλλεται αναλόγως. Όταν ικανοποιηθούμε με την αλλαγή, δίνουμε ξανά [$mod + R] κι ο i3 παύει να ερμηνεύει το πάτημα των arrow keys ως εντολές αλλαγής μεγέθους.

Τι κάνουμε άραγε αν το τρέχον workspace (σκεφτείτε "desktop") έχει πολλά ανοικτά παράθυρα και η εργασία σε αυτό δεν είναι πλέον τόσο άνετη; Κατ' αρχάς, με ένα συνδυασμό πλήκτρων της μορφής [$mod + #], όπου το # είναι ακέραιος μεταξύ 0 κι 9, δημιουργούμε ένα νέο workspace (το 0 αντιστοιχεί στο workspace υπ' αριθμόν 10). Σε κάθε workspace μπορούμε, φυσικά, να έχουμε ανοικτά όσα κι όποια παράθυρα θέλουμε. Επίσης, ένα παράθυρο που έχει το focus το μεταφέρουμε σε άλλο workspace πατώντας ένα συνδυασμό πλήκτρων της μορφής [$mod + Shift + #], όπου το # είναι ακέραιος μεταξύ 0 και 9 (και το 0 αντιστοιχεί πάντα στο workspace 10).

Τέλος, όταν κάποια στιγμή θελήσουμε να βγούμε από τον i3 (λέμε τώρα) τότε αρκεί να πατήσουμε το συνδυασμό πλήκτρων [$mod + Shift + E]. Στο πάνω μέρος της οθόνης θα εμφανιστεί μια οριζόντια (πορτοκαλί) μπάρα, όπου καλούμαστε να επιβεβαιώσουμε ή να ακυρώσουμε την εντολή αποσύνδεσης.

Σημείωση. Όπως προαναφέραμε, ο i3 ανήκει στην κατηγορία των dynamic window managers κι αυτό σημαίνει ότι έχει τη δυνατότητα να συμπεριφέρεται είτε ως floating είτε ως tiling window manager. Εξ ορισμού συμπεριφέρεται ως tiling, αλλά αυτό αλλάζει εύκολα από το configuration file. Έχετε επίσης κατά νου ότι σε συγκεκριμένες περιπτώσεις παρουσιάζει συμπεριφορά floating window manager αυτόματα, από μόνος του. Για παράδειγμα, τα "Save As" dialogs ή τα toolbars εφαρμογών όπως το Gimp, έχει πολύ περισσότερο νόημα να εμφανίζονται ως floating windows παρά ως tiles. Στον i3, τα floating windows παραμένουν πάντα πάνω από όλα τα tiled windows.

Ρύθμιση του i3 WM

Τη συμπεριφορά αλλά και την όψη του i3 τα τροποποιούμε επεμβαίνοντας στο configuration file με όνομα config, κάτω από τον κατάλογο ~/.config/i3 (το πλήρες path του αρχείου ρυθμίσεων, δηλαδή, είναι ~/.config/i3/config). Μια άλλη θέση του config που ίσως ισχύει για τη διανομή σας, είναι κάτω από τον κατάλογο ~/.i3 (το full path, δηλαδή, θα είναι ~/.i3/config). Το configuration file το ανοίγουμε με κάποιον text editor όπως, π.χ., vi, nano, gedit κ.ά. Οι όποιες αλλαγές κάνουμε λαμβάνονται υπόψη αποθηκεύοντας κι επανεκκινώντας τον i3 επιτόπου, με ένα [$mod + Shift + R]. Αν υπάρχει κάποιο λάθος στο αρχείο ρυθμίσεων, λαμβάνουμε σχετική προειδοποίηση. Να πούμε επίσης ότι ανά πάσα στιγμή μπορούμε να επαναφέρουμε το πρωτότυπο (αρχικό) config διαγράφοντας το υπάρχον κι αμέσως μετά, σε ένα τερματικό, πληκτρολογώντας `i3-config-wizard`. Ανοίξτε τώρα το configuration file και ρίξτε μια ματιά στο περιεχόμενό του. Θα διαπιστώσετε ότι οι αποδεκτές οδηγίες/ρυθμίσεις είναι απλές και κατανοητές — και σε αυτό βοηθούν τα επεξηγηματικά σχόλια. Στη συνέχεια παρουσιάζουμε τις επεμβάσεις που έχουμε κάνει στο δικό μας config. Δεν είναι υποχρεωτικό να κάνετε ακριβώς τις ίδιες, φυσικά.

Γραμματοσειρά για τους τίτλους των παραθύρων. Η προκαθορισμένη γραμματοσειρά (και το μέγεθός της) για τους τίτλους των παραθύρων, ίσως να μη σας αρέσει. Η προεπιλογή έχει ως εξής:

```
font pango:monospace 8
```

Στη εκδοχή του config που έχουμε στο σύστημα των δοκιμών χρησιμοποιούμε τη γραμματοσειρά Roboto Mono, με μέγεθος 11:

```
font pango:robotomono 11
```

Τη συγκεκριμένη γραμματοσειρά βρήκαμε κι εγκαταστήσαμε από το Google Fonts (https://fonts.google.com).

Προεπιλεγμένη εφαρμογή τερματικού. Εξ ορισμού, όταν πατάμε το συνδυασμό πλήκτρων [$mod + Enter] εκτελείται το script ονόματι `i3-sensible-terminal`. Δουλειά του είναι να εντοπίζει την πρώτη διαθέσιμη εφαρμογή τερματικού και να την τρέχει. Αν τώρα έχετε κάποιον αγαπημένο terminal emulator και θέλετε να ενεργοποιείται αυτός χωρίς περιττές αναζητήσεις, αλλάξτε κατάλληλα την ακόλουθη οδηγία:

```
bindsym $mod+Return exec i3-sensible-terminal
```

Σε εμάς, π.χ., αυτόν τον καιρό αρέσει πολύ το GNOME Terminal, οπότε στο config του i3 έχουμε την ακόλουθη οδηγία:

```
bindsym $mod+Return exec gnome-terminal --hide-menubar
```

Παρατηρήστε την παράμετρο `--hide-menubar`, χάρη στην οποία το GNOME Terminal ξεκινά χωρίς την πάνω οριζόντια μπάρα. Το περιβάλλον του i3 είναι λιτό και θέλουμε να το διατηρούμε λιτό πάση θυσία.

Key bindings εκκίνησης εφαρμογών. Το `htop` είναι μια εφαρμογή για την κονσόλα απλού κειμένου που συχνά-πυκνά εκτελούμε. Γι' αυτό και στο configuration file του i3 έχουμε την ακόλουθη οδηγία:

```
bindsym $mod+t exec gnome-terminal -e /usr/bin/htop
```

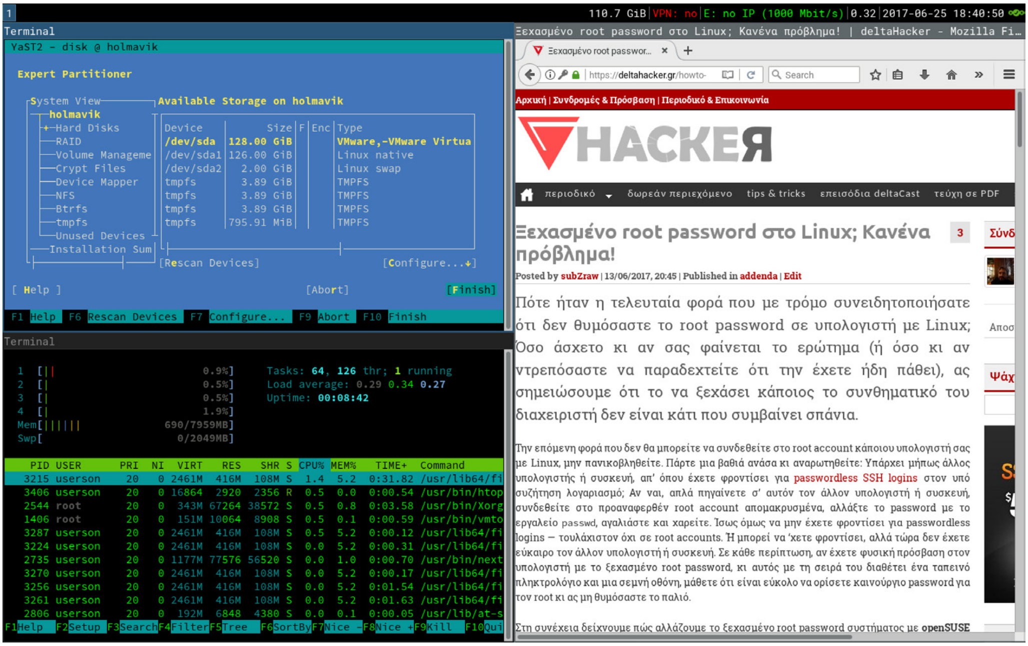
Κάθε φορά που πατάμε τον συνδυασμό πλήκτρων [$mod + T], λοιπόν, ανοίγει ένα GNOME Terminal με το htop να τρέχει εντός. Μια άλλη εφαρμογή που τρέχουμε από καιρού εις καιρόν είναι το YaST2. Χάρη στην οδηγία

```
bindsym $mod+y exec gnome-terminal -e "sudo /usr/sbin/yast2"
```

κάθε φορά που πατάμε [$mod + Y] ανοίγει ένα GNOME Terminal, με το YaST2 να τρέχει εντός. Παρατηρήστε και τη χρήση του sudo, αφού το YaST2 πρέπει να τρέχει με δικαιώματα διαχειριστή.

Καθορισμός wallpaper. Όταν συνδεόμαστε στο περιβάλλον του i3 δεν υπάρχει κάποιο wallpaper. Μπορείτε βεβαίως να καθορίσετε μια εικόνα που προτιμάτε, ώστε κατά το φόρτωμα του i3 να μπαίνει ως wallpaper. Παράδειγμα:

```
exec --no-startup-id /usr/bin/feh --bg-scale ~/Pictures/opensuse-green-
lightbulb.jpg
```



Το αριστερό μισό του workspace μοιράζονται δύο εφαρμογές (YaST2 και htop) για τις οποίες, παρεμπιπτόντως, έχουμε ορίσει αντίστοιχα key bindings. Το δεξιό μισό του workspace έχει καταλάβει αποκλειστικά ο Firefox.

Όπως βλέπετε, χρησιμοποιούμε το εργαλείο feh και μάλιστα με την παράμετρο --bg-scale, ώστε το μέγεθος της εικόνας να προσαρμόζεται αυτομάτως στο workspace.

Καθορισμός ανάλυσης οθόνης. Ο i3 είναι σε θέση να εντοπίζει από μόνος του τη σωστή ανάλυση της οθόνης. Κατά περιπτώσεις όμως ίσως θα αποτυγχάνει, ειδικά αν δοκιμάζετε τον i3 σε εικονικό υπολογιστή. Τότε, καλό είναι να χρησιμοποιούμε το εργαλείο xrandr (χωρίς καμία παράμετρο), ώστε αφενός να μάθουμε το όνομα του display καθώς και τις αναλύσεις που υποστηρίζει. Στο VM μας, το όνομα του display είναι Virtual1 και η φυσική ανάλυση της οθόνης είναι 1440x900 εικονοστοιχεία. Έτσι, στο configuration file του i3 έχουμε την ακόλουθη γραμμή:

```
exec xrandr --output Virtual1 --mode 1440x900
```

Καθορισμός θέσης και πληροφοριών για την i3bar. Η μπάρα του i3 εμφανίζεται στο κάτω μέρος της οθόνης. Αν θέλετε να της αλλάξετε θέση, ώστε να είναι στο πάνω μέρος της οθόνης, βρείτε την ενότητα

```
bar {
        status_command i3status
}
```

και προσθέστε οδηγία για τη θέση:

```
bar {
      position top
      status_command i3status
}
```

Είναι νομίζουμε προφανές ότι στη μπάρα του i3 εμφανίζονται οι πληροφορίες που επιστρέφει το utility ονόματι i3status. Οι πληροφορίες που συλλέγει το εν λόγω εργαλείο καθορίζονται στο αρχείο /etc/i3status.conf. Ίσως θελήσετε να το τροποποιήσετε ελαφρώς, ώστε, π.χ., να μην εμφανίζονται πληροφορίες περί IPv6 ή ό,τι άλλο θεωρείτε περιττό.

Αυτόματη εκκίνηση εφαρμογών. Κατά την εκκίνηση του i3 είναι πολύ πιθανό να επιθυμούμε την εκτέλεση συγκεκριμένων εφαρμογών. Εμείς για παράδειγμα θέλουμε να ξεκινά ο επίσημος Nextcloud client, για τον Nextcloud server που έχουμε σε ένα Raspberry Pi 3 (https://deltahacker.gr/?p=17061). Γι' αυτό και στο config του i3 έχουμε την ακόλουθη γραμμή:

```
exec /usr/bin/nextcloud
```

Εικονίδια εφαρμογών σαν το Nextcloud client, εμφανίζονται στα δεξιά της i3bar.

Keyboard layout. Ανά πάσα στιγμή θέλουμε να αλλάζουμε layout στο πληκτρολόγιο, επιλέγοντας μεταξύ Αγγλικών κι Ελληνικών με το πρώτο να είναι το προεπιλεγμένο. Η αλλαγή layout μας βολεύει να γίνεται πατώντας [Alt + Shift], γι' αυτό και στο configuration file του i3 έχουμε τις ακόλουθες δύο γραμμές:

```
exec setxkbmap -layout us,gr
exec setxkbmap -option 'grp:alt_shift_toggle'
```

Προκειμένου να ληφθούν υπόψη τώρα οι ρυθμίσεις περί layout, δεν επανεκκινούμε τον i3 (με [$mod + Shift + R]). Αντίθετα, σε ένα τερματικό γράφουμε διαδοχικά:

```
setxkbmap -layout us,gr
setxkbmap -option 'grp:alt_shift_toggle'
```

Μια εναλλακτική για το dmenu

Χάρη στο dmenu, η εκτέλεση εφαρμογών με GUI επιτυγχάνεται εύκολα μέσα από τον i3. Πιθανώς όμως να βρίσκετε κάπως άσχημη την οριζόντια μπάρα που εμφανίζεται στο πάνω μέρος της οθόνης, κάθε φορά που πατάτε [$mod + D]. Ένα εναλλα-

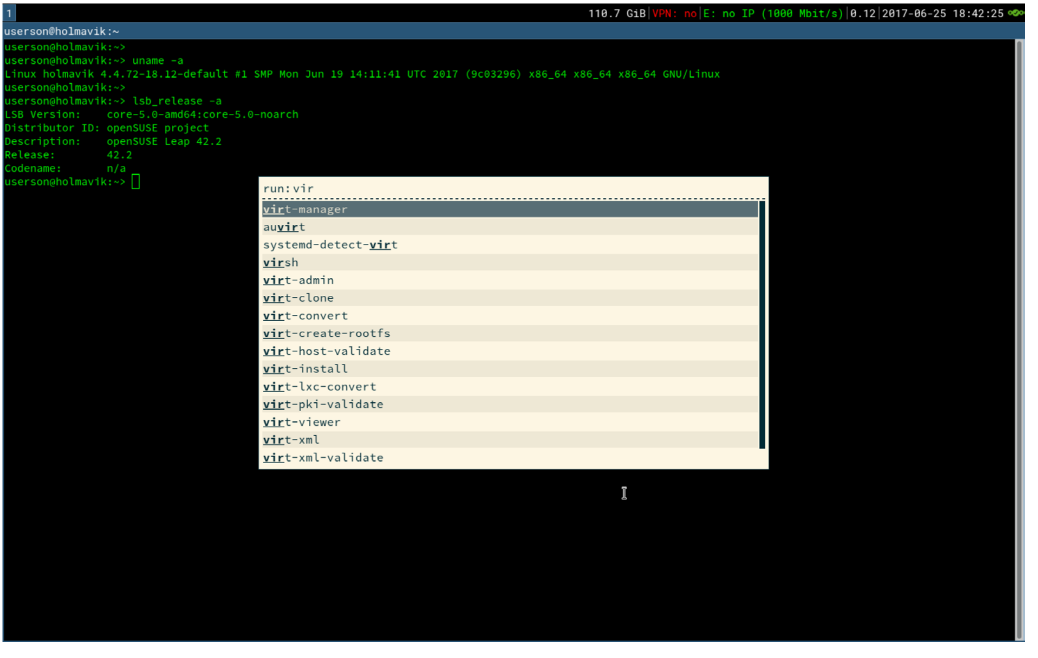
κτικό του dmenu εργαλείο είναι το rofi. Στο openSUSE το εγκαθιστούμε πληκτρολογώντας `zypper in rofi` (με δικαιώματα root). Μετά, ανοίγουμε το configuration file του i3 κι αλλάζουμε τη γραμμή

```
bindsym $mod+d exec dmenu_run
```

ώστε να γίνει όπως η ακόλουθη:

```
bindsym $mod+d exec rofi -show run
```

Πατήστε τώρα το συνδυασμό πλήκτρων [$mod + D] και δείτε το νέο interface για την εκτέλεση εφαρμογών. Το rofi είναι λιγότερο διακριτικό σε σύγκριση με το dmenu, σε εμάς όμως αρέσει περισσότερο. Θα μας ενδιέφερε να μας δώσετε το feedback σας για τον ίδιο τον i3. Πώς σας φαίνεται; Έχει πιθανότητες να αποτελέσει το default desktop environment για το Linux σας; Αιτιολογήστε, παρακαλούμε, την όποια απάντησή σας.



Μπορεί το rofi να είναι λιγότερο διακριτικό από το dmenu, για εμάς όμως αποτελεί ένα άριστο εργαλείο για την εκτέλεση εφαρμογών.

Skill: Intermediate
Tags: Kali Linux, OpenVAS, vulnerabilities, scanner

Ανίχνευση αδυναμιών με το καινούργιο OpenVAS

Προς τα τέλη του περασμένου Απριλίου κυκλοφόρησε η πιο πρόσφατη έκδοση του Kali, της δημοφιλούς διανομής Linux για digital forensics και penetration testing. Μεταξύ των ανανεωμένων χαρακτηριστικών του Kali Linux είναι η συμπερίληψη του OpenVAS 9 στα repositories της διανομής.

Το Open Vulnerability Assessment System, εν συντομία OpenVAS, είναι μια ευέλικτη πλατφόρμα για την ανίχνευση και τη διαχείριση αδυναμιών ασφαλείας σε συστήματα. Με το OpenVAS είχαμε ασχοληθεί τρία και πλέον χρόνια πριν, αναπτύσσοντας αναλυτικά άρθρα στο περιοδικό (βλ. τεύχος 028, https://deltahacker.gr/deltahacker028) αλλά κι εκτενές video tutorial (βλ. deltaCast s02e01, https://deltahacker.gr/?p=10572). Αρκετά έχουν αλλάξει από τότε, ώστε να έχει νόημα να δούμε ξανά το OpenVAS με μια φρέσκια ματιά.

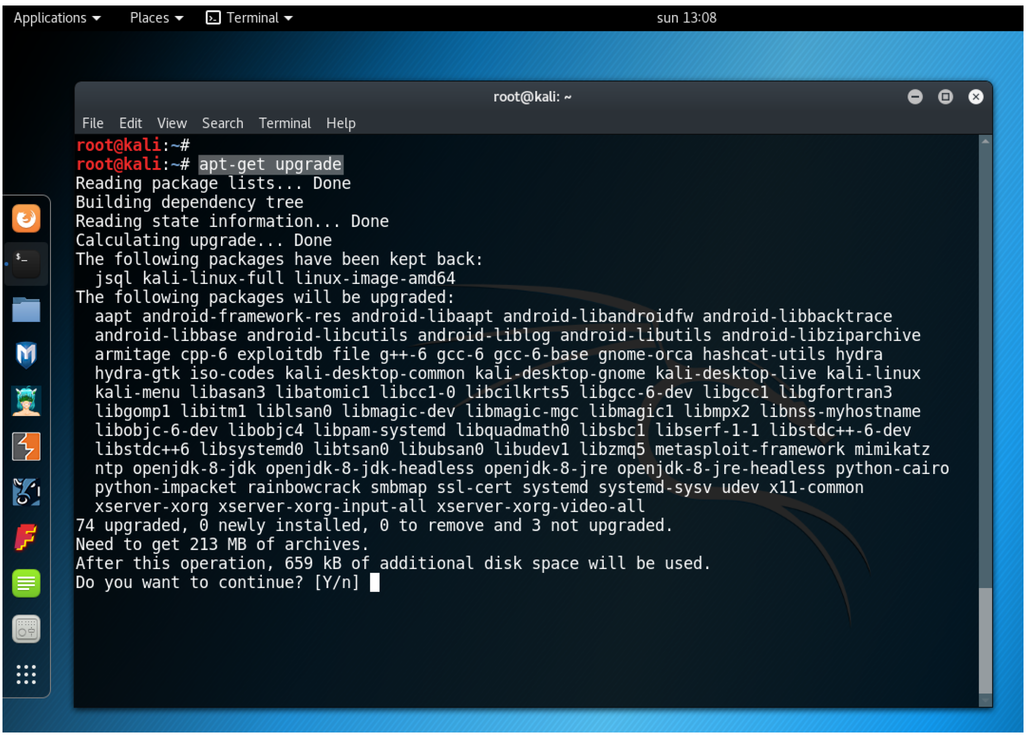
Απαραίτητη προετοιμασία

Όπως είπαμε, θα παίξουμε με το OpenVAS μέσα από το καινούργιο Kali Linux. Από την επίσημη σελίδα download της διανομής (https://www.kali.org/downloads) επιλέξτε την εκδοχή που προτιμάτε και κατεβάστε τη. Εμείς, π.χ., πήραμε εκείνη με το περιβάλλον γραφικών του GNOME, για συστήματα με επεξεργαστή αρχιτεκτονικής x86-64. Ιδού το σχετικό torrent → https://images.offensive-security.com/kali-linux-2017.1-amd64.torrent κι εδώ είναι και το link για direct downloading → http://cdimage.kali.org/kali-2017.1/kali-linux-2017.1-amd64.iso. Σε κάθε περίπτωση, μετά τη λήψη θα έχετε το ISO image του Kali Linux 2017.1. Αν δεν σκοπεύετε να το εγκαταστήσετε σε εικονικό αλλά σε φυσικό υπολογιστή, τότε προτείνουμε να περάσετε το ISO σε USB stick (https://deltahacker.gr/iso2usb) και να ξεκινήσετε τον υπολογιστή απ' αυτό.

Η περιγραφή της διαδικασίας εγκατάστασης του Kali ξεφεύγει από τους σκοπούς του παρόντος. Σημειώνουμε μόνο ότι μετά το πέρας της –και σίγουρα πριν στρέψουμε την προσοχή μας στο OpenVAS 9–, καλό είναι να φρεσκάρουμε τα repositories της διανομής και μετά να εφαρμόσουμε τις όποιες διαθέσιμες αναβαθμίσεις:

```
root@kali:~# apt-get update
root@kali:~# apt-get upgrade
```

Αναλόγως του χρόνου που έχει μεσολαβήσει από το προηγούμενο upgrade, η διαδικασία ενδέχεται να ολοκληρωθεί σε δευτερόλεπτα έως αρκετά λεπτά.

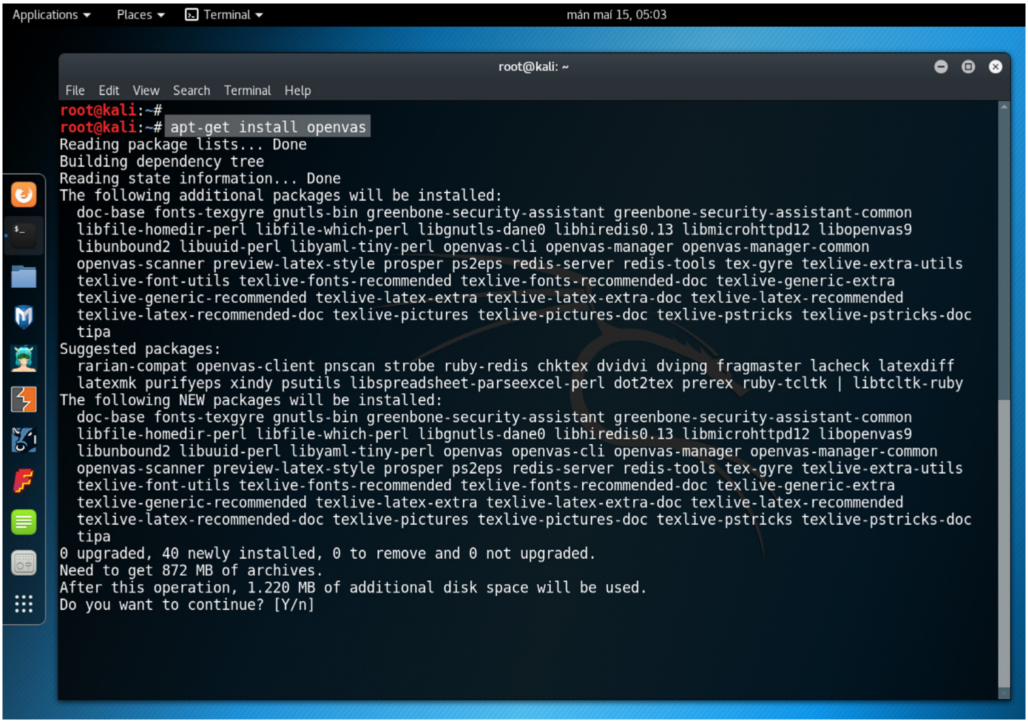


Δεν είναι και λίγες οι διαθέσιμες αναβαθμίσεις για την εγκατάσταση του Kali που τρέχουμε. Μετά την ολοκλήρωση της διαδικασίας, προσέξτε για την περίπτωση που έχει αναβαθμιστεί κι ο πυρήνας του λειτουργικού. Αν πράγματι έχει, κάντε μια επανεκκίνηση.

Εγκατάσταση OpenVAS 9 και σύνδεση στο web panel

Όπως αναφέραμε ήδη, η καινούργια έκδοση του OpenVAS βρίσκεται στα αποθετήρια λογισμικού (software repositories) του Kali Linux 2917.1. Για την εγκατάσταση, λοιπόν, αρκεί να πληκτρολογήσουμε:

```
root@kali:~# apt-get install openvas
```

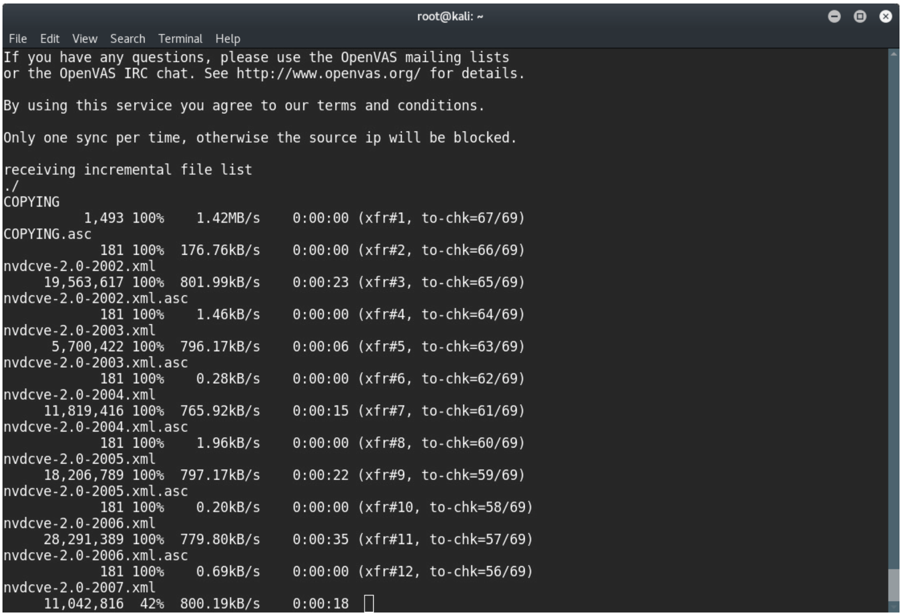


Το OpenVAS χρειάζεται αρκετά άλλα πακέτα για να λειτουργήσει σωστά. Για παράδειγμα, το συνολικό μέγεθος των πακέτων για τη δική μας εγκατάσταση έφτανε τα 872MB. Όλες αυτές τις εξαρτήσεις (dependencies) τις τακτοποιεί το apt. Από τη μεριά μας δεν έχουμε παρά να δεχτούμε την πρότασή του, για τα πακέτα που πρέπει να εγκατασταθούν.

Όταν η διαδικασία της εγκατάστασης ολοκληρωθεί, πληκτρολογούμε:

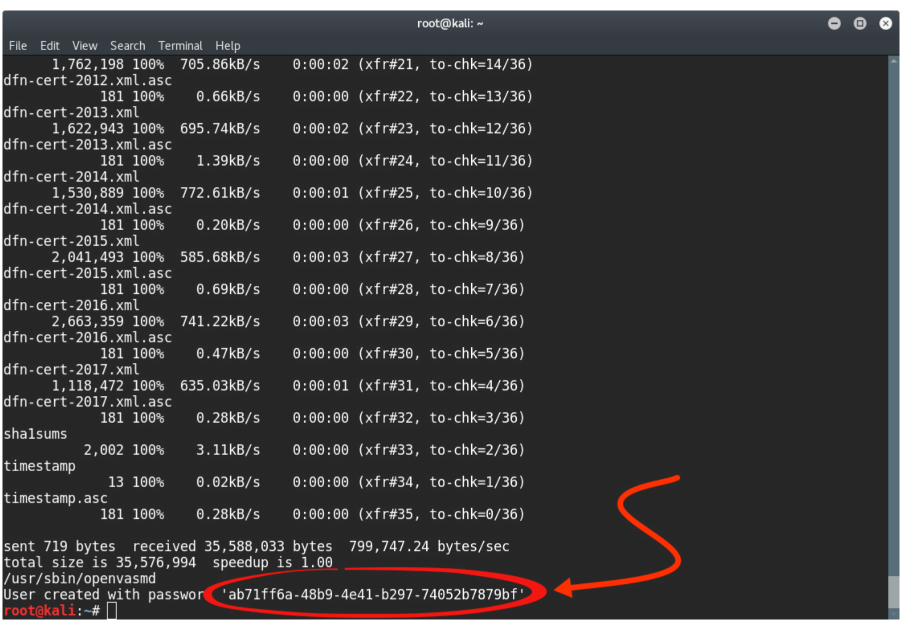
```
root@kali:~# openvas-setup
```

Το εργαλείο openvas-setup **α)** κατεβάζει μια υπερπληθώρα από Network Vulnerability Tests (NVTs), με βάση τα οποία η πλατφόρμα είναι σε θέση να αναγνωρίζει αδυναμίες, **β)** δημιουργεί ένα χρήστη με δικαιώματα διαχειριστή (για το OpenVAS, όχι για το Kali), ενώ **γ)** ξεκινά και τις υπηρεσίες (services) που χρειάζεται το OpenVAS προκειμένου να λειτουργεί σωστά. Έχετε υπόψη ότι *ειδικά* την πρώτη φορά που θα τρέξετε το openvas-setup, θα χρειαστεί αρκετό χρόνο για να ολοκληρώσει τις εργασίες του. Γενικά, ο χρόνος αυτός είναι πρωτίστως ανάλογος της ταχύτητας της ιντερνετικής σας σύνδεσης. Δευτερευόντως, εξαρτάται από τους πόρους του εικονικού/φυσικού υπολογιστή με το Kali.



Την πρώτη φορά που θα το τρέξουμε, το openvas-setup θα χρειαστεί αρκετό χρόνο πριν ολοκληρώσει τις εργασίες του.

Αφού το openvas-setup τελειώσει τις δουλειές του, μας δείχνει το password που έχει αντιστοιχίσει στο χρήστη admin. Το συγκεκριμένο συνθηματικό το χρειαζόμαστε προκειμένου να συνδεθούμε στο web panel της πλατφόρμας.



Δεν το λες κι αδύναμο το password που έχει βάλει στο λογαριασμό του χρήστη admin, το openvas-setup. Σημειώστε το κάπου γιατί σε λίγο θα το χρειαστείτε – αλλά έχετε κι υπόψη ότι μπορείτε να ορίσετε το δικό σας password.

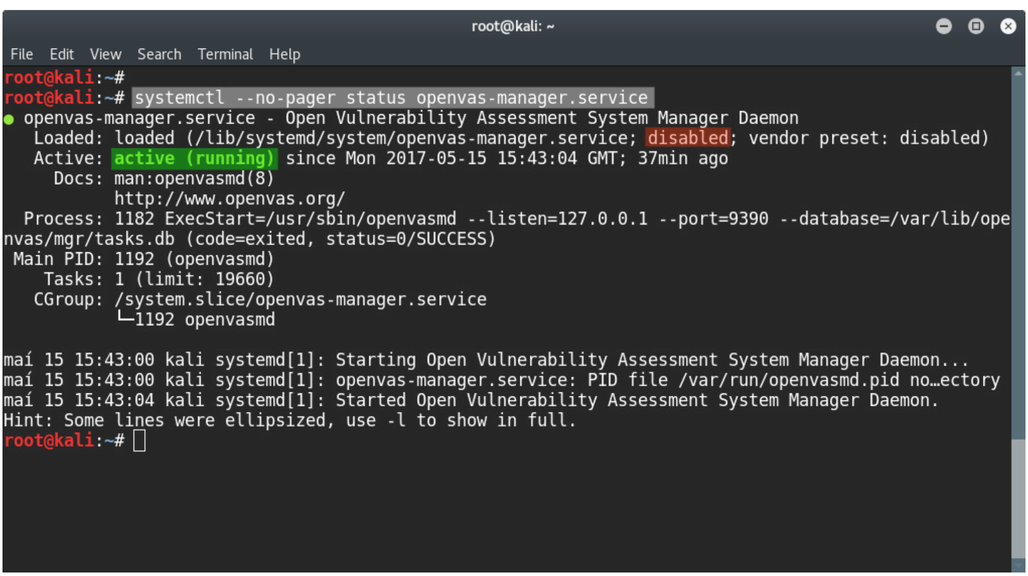
Αν το αυτόματα δημιουργημένο password σάς φαίνεται περιττά περίπλοκο –ή τέλος πάντων θέλετε να ορίσετε το δικό σας–, αλλάξτε το με το εργαλείο openvasmd:

```
root@kali:~# openvasmd --user=admin --new-password=eyjafjallajokull
```

Όπως είπαμε πριν λίγο, το openvas-setup ξεκινά συγκεκριμένες υπηρεσίες που είναι απαραίτητες για τη λειτουργία της πλατφόρμας. Οι υπηρεσίες αυτές είναι οι ακόλουθες τρεις:

- **openvas-manager**, υπηρεσία διαχείρισης των user configurations καθώς και των αποτελεσμάτων που παράγουν οι σαρώσεις, πρακτικά στέκεται ανάμεσα σε χρήστες και scanners
- **openvas-scanner**, η μηχανή που πραγματοποιεί τα network vulnerability tests
- **greenbone-security-assistant**, παρέχει πρόσβαση στον Greenbone Security Assistant, ένα εύχρηστο web panel για το OpenVAS

Αν με το εργαλείο systemctl ζητήσετε να δείτε το status καθεμιάς εκ των προαναφερθέντων υπηρεσιών, θα διαπιστώσετε ότι αν και είναι ενεργή (active ή running) την ίδια στιγμή είναι απενεργοποιημένη (disabled). Δείτε το ακόλουθο screenshot.



Το openvas-setup φροντίζει και ξεκινά τις υπηρεσίες που το OpenVAS χρειάζεται, δεν τις ενεργοποιεί όμως (στην εικόνα φαίνεται μία από τις τρεις υπηρεσίες).

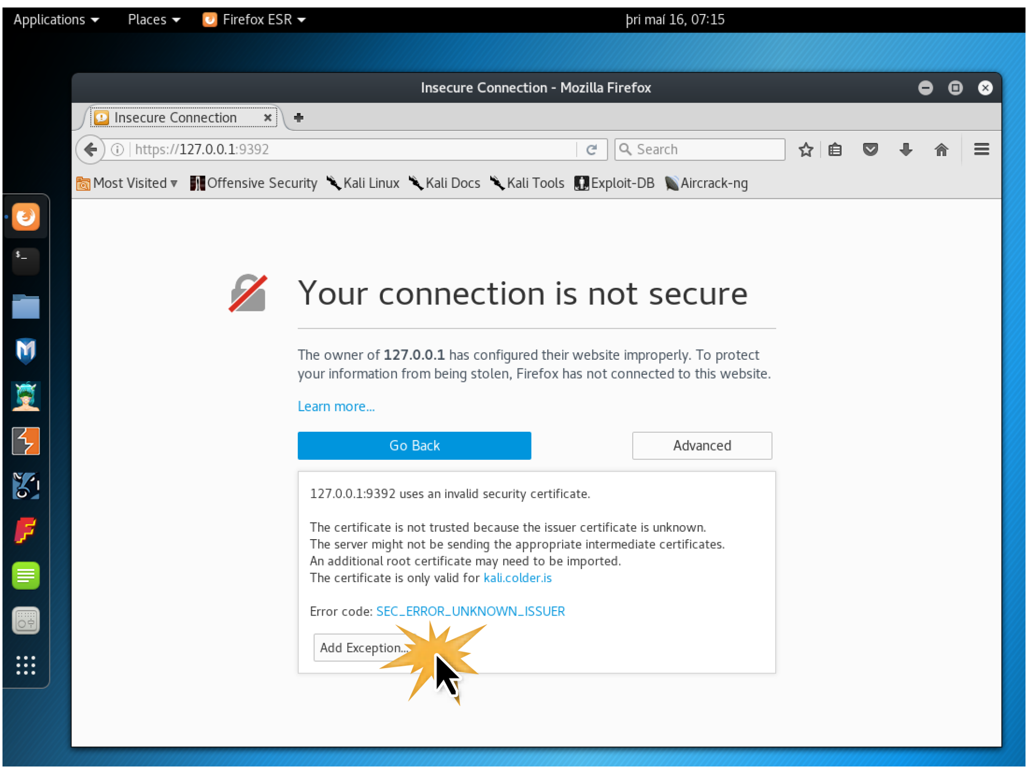
Περισσότερα για το systemd και τη διαχείριση υπηρεσιών μπορείτε να διαβάσετε στο https://deltahacker.gr/systemd-and-logging. Γενικά, δεν υπάρχει λόγος ώστε οι υπηρεσίες openvas-manager, openvas-scanner και greenbone-security-assistant να

είναι ενεργοποιημένες – εκτός κι αν πρόκειται να δουλεύετε με το OpenVAS τακτικά. Για την ευκολία μας, πάντως, μετά από κάθε (επαν)εκκίνηση του Kali μπορούμε να ξεκινάμε *χειροκίνητα* τις τρεις αυτές υπηρεσίες με μία μόνο εντολή:

```
root@kali:~# openvas-start
```

Για τη σύνδεση στο web panel του OpenVAS, από έναν web browser αρκεί να επισκεφτούμε τη διεύθυνση https://127.0.0.1:9392. Την πρώτη φορά θα λάβουμε ειδοποίηση για self-signed πιστοποιητικό, δημιουργούμε όμως μια εξαίρεση στον browser και συνεχίζουμε.

Μπορούμε τώρα να συνδεθούμε στο web panel – και συγκεκριμένα στο λογαριασμό του χρήστη με username το admin. Το password είναι είτε αυτό που ετοίμασε για εμάς το openvas-setup, είτε εκείνο που ορίσαμε με την εντολή openvasmd. Αφού λοιπόν συνδεθούμε, σίγουρα θα θέλουμε να κάνουμε το πρώτο μας scan για vulnerabilities. Πώς ακριβώς δουλεύουμε;



Το πιστοποιητικό για το web panel του OpenVAS (Greenbone Security Assistant) είναι self-signed, γι' αυτό κι ο Firefox διαμαρτύρεται. Δημιουργώντας μια εξαίρεση δεν βλέπουμε ξανά ανάλογες ειδοποιήσεις – τουλάχιστον όχι για το συγκεκριμένο site.

Κυνήγι αδυναμιών με το OpenVAS 9

Ο καλύτερος τρόπος προκειμένου να μάθουμε το OpenVAS αλλά και να εκτιμήσουμε τις δυνατότητες και τους περιορισμούς του, είναι να δούμε, αναλυτικά και βήμα προς βήμα, πώς σκανάρουμε ένα σύστημα για αδυναμίες. Σε γενικές γραμμές η πρώτη μας δουλειά είναι να ορίσουμε ένα target, μ' άλλα λόγια ένα ή περισσότερα μηχανήματα που θέλουμε να σκανάρουμε. Μετά τον ορισμό target ορίζουμε κι ένα task, το οποίο χρησιμοποιεί το προαναφερθέν target προκειμένου να τρέξει μια σειρά από network vulnerability tests.

Το OpenVAS κάλλιστα μπορεί και σκανάρει απομακρυσμένα hosts στο Internet, όσο και τοπικά hosts εντός του LAN. Καλό είναι πάντως να μη σκανάρουμε απομακρυσμένα hosts, εκτός κι αν έχουμε πάρει σχετική άδεια από τους υπευθύνους. Ας δούμε λοιπόν πώς ψάχνουμε για αδυναμίες σε ένα host μέσα από το LAN, στο οποίο βρίσκεται και το Kali Linux μας. Ένας γρήγορος κι αξιόπιστος τρόπος για να βρίσκουμε τις διευθύνσεις IP όλων των hosts που είναι ενεργά εντός του LAN, είναι με χρήση του εργαλείου netdiscover:

```
root@kali:~# netdiscover -P -r 192.168.193.0/24
```

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~#
root@kali:~# netdiscover -P -r 192.168.193.0/24

 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.193.1   00:50:56:c0:00:02      1      60  Unknown vendor
 192.168.193.235 00:0c:29:ce:d6:3c      1      60  Unknown vendor
 192.168.193.242 00:0c:29:71:71:b8      1      60  Unknown vendor
 192.168.193.254 00:0c:29:8b:ff:e8      1      60  Unknown vendor

-- Active scan completed, 4 Hosts found.
root@kali:~#
root@kali:~# 
```

Ανίχνευση ενεργών hosts εντός του τοπικού δικτύου που βρίσκεται το Kali Linux. Τα μηχανήματα του LAN παίρνουν διευθύνσεις IP της μορφής 192.168.193..*

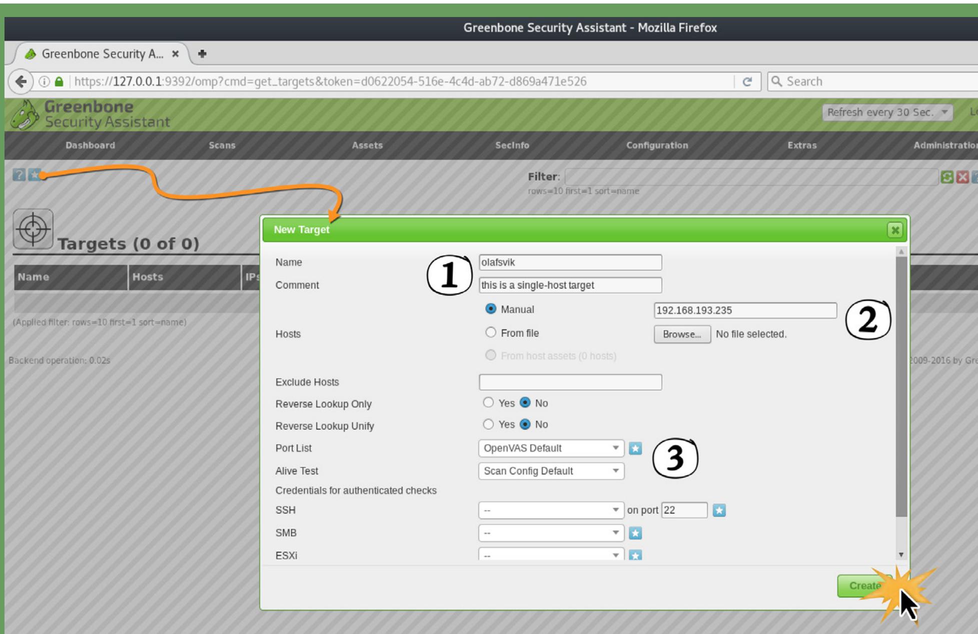
Από τα μηχανήματα που εντόπισε το netdiscover, ας σκανάρουμε εκείνο με IP το 192.168.193.235 (τρέχει Linux). Αν στο σημείο αυτό θέλουμε να κάνουμε κι ένα reverse DNS lookup, ώστε να βρούμε το FQDN (Fully Qualified Domain Name) του μηχανήματος-στόχου, αρκεί να πληκτρολογήσουμε:

```
root@kali:~# dig -x 192.168.193.235 +short
```

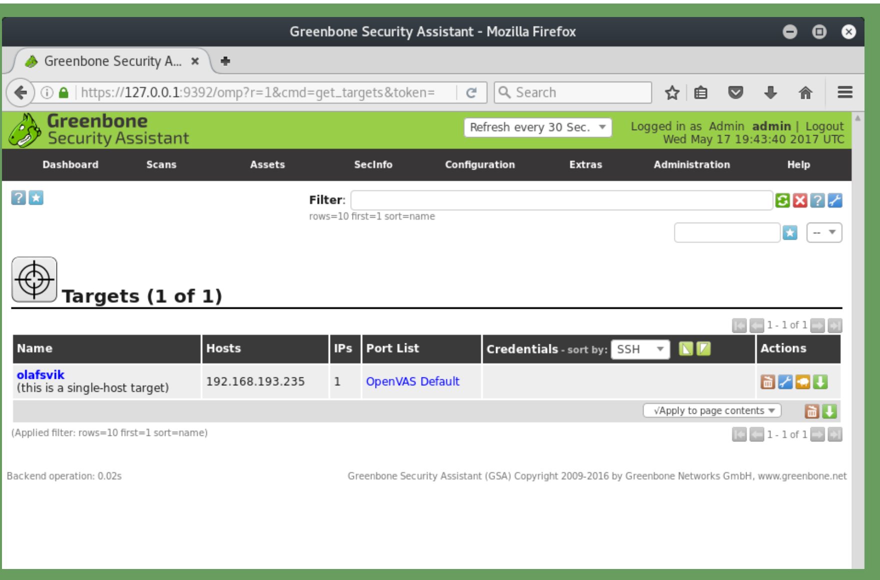


Παράδειγμα reverse DNS lookup με το εργαλείο dig. Στο τοπικό μας δίκτυο, το FQDN του 192.168.193.235 είναι olafsvik.colder.is. Παρεμπιπτόντως, το λειτουργικό σύστημα του host είναι κάποια διανομή του Linux.

Στρέφουμε την προσοχή μας στο web panel του OpenVAS. Φτιάχνουμε ένα νέο target επιλέγοντας Configuration / Targets. Στη σελίδα που εμφανίζεται κάνουμε κλικ στο γαλάζιο εικονίδιο με το λευκό αστερίσκο, πάνω αριστερά. Παρουσιάζεται τότε ένα pop-up με όνομα New Target. Δείτε τα δύο screenshots που ακολουθούν, διαβάστε και τις αντίστοιχες περιγραφές.

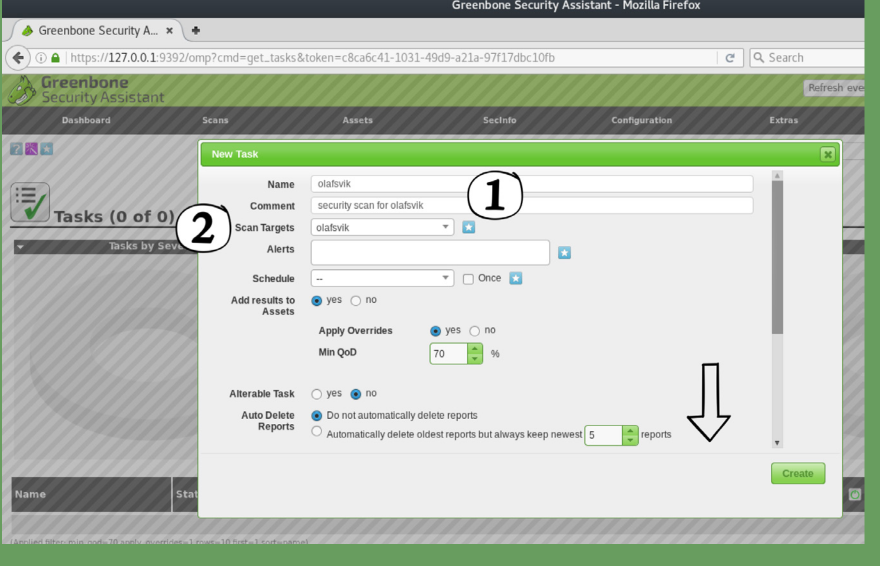


Για το νέο μας στόχο πληκτρολογούμε ένα όνομα, καθώς και μια κατάλληλη περιγραφή (1). Στην περιοχή Hosts, από κάτω, αφήνουμε επιλεγμένο το Manual και στη θυρίδα δεξιά γράφουμε τη διεύθυνση IP του στόχου (2). Παρατηρήστε ότι υπάρχει δυνατότητα καθορισμού πολλών στόχων μαζί, οι διευθύνσεις των οποίων παρατίθενται σε αρχείο (βλ. From file). Για την πρώτη μας δοκιμή, τέλος, στις παραμέτρους Port List και Alive Test αφήνουμε τις προεπιλεγμένες τιμές (3). Ο καθορισμός του στόχου ολοκληρώνεται με ένα κλικ στο κουμπί Create, κάτω δεξιά.



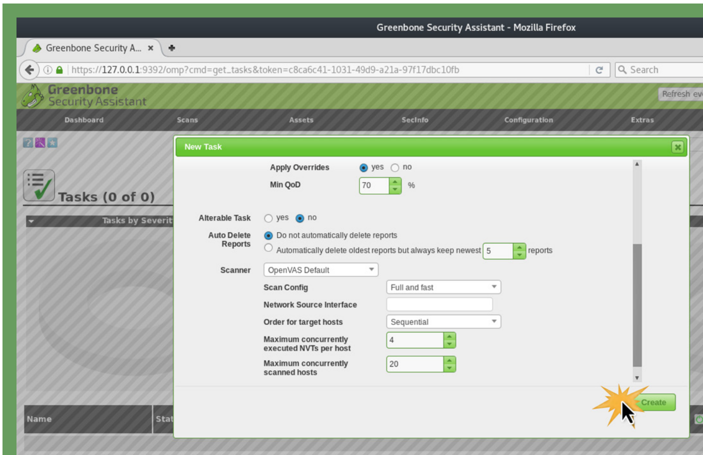
Ιδού οι στόχοι που έχουμε καθορίσει. Εντάξει, προς το παρόν έχουμε μόνον έναν.

Μετά τον ορισμό target έχουμε να ορίσουμε κι ένα task που θα αφορά στο target. Στο web panel του OpenVAS επιλέγουμε Scans / Tasks. Εμφανίζεται ένα πληροφοριακό pop-up, το οποίο παραμένει για δέκα δευτερόλεπτα (δεν χρειάζεται φυσικά να περιμένουμε, πατάμε στο [x] πάνω δεξιά και το κλείνουμε). Για άλλη μια φορά πατάμε στο εικονίδιο με τον αστερίσκο, πάνω αριστερά. Δείτε τα επόμενα screenshots.

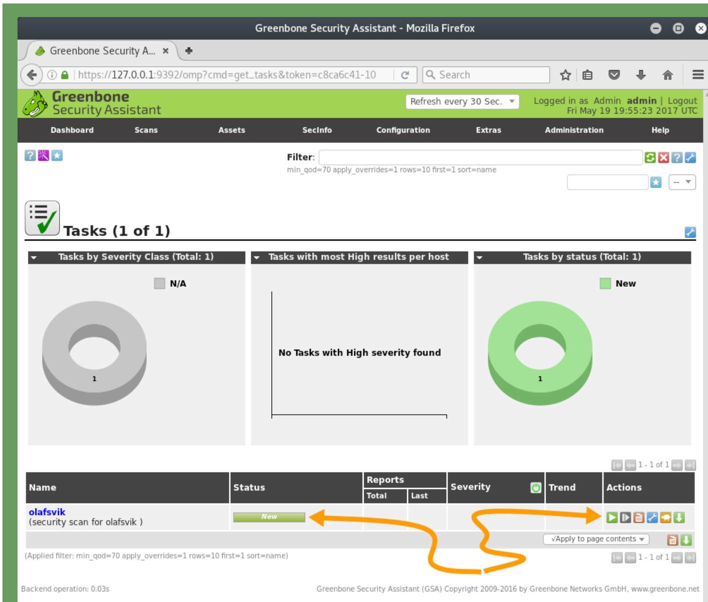


Για τη νέα μας εργασία πληκτρολογούμε ένα χαρακτηριστικό όνομα και μια περιγραφή (1). Στο πεδίο Scan Targets επιλέγουμε το στόχο ή τους στόχους στους

οποίους αφορά η εργασία (2). Προς το παρόν διαθέτουμε έναν μόνο στόχο – και στο πλαίσιο της παρουσίασής μας τον έχουμε ονομάσει olafsvik. Για όλες τις άλλες παραμέτρους αφήνουμε τις προκαθορισμένες τιμές. Σκρολάρουμε λίγο προς τα κάτω, ώστε να δούμε και τα υπόλοιπα περιεχόμενα του παραθύρου New Task.



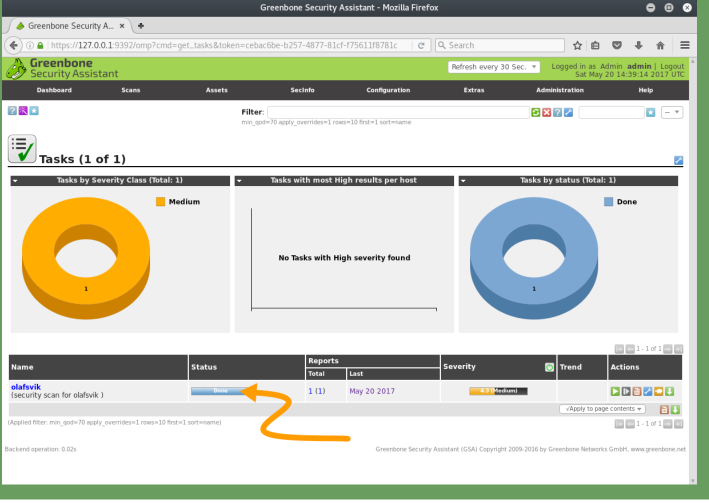
Δείτε λίγο τις τιμές που επιδέχονται οι παράμετροι Scanner και Scan Config. Για αρχή, πάντως, μπορείτε να αφήσετε τις προεπιλεγμένες. Η νέα εργασία δημιουργείται με ένα κλικ στο κουμπί Create, κάτω δεξιά.



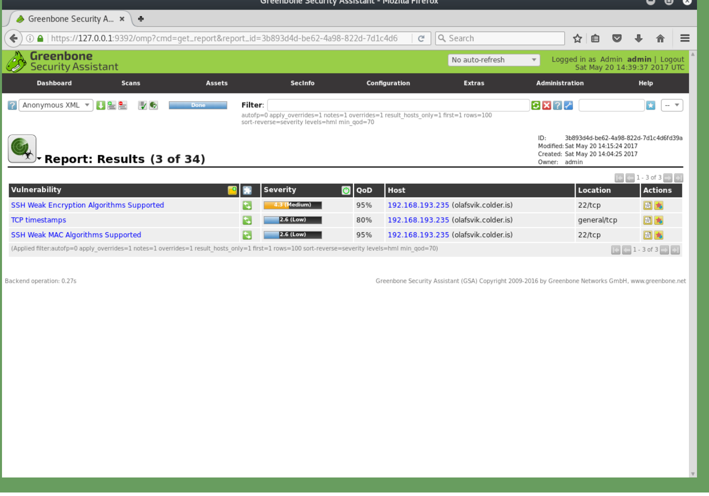
Το πρώτο μας task, το οποίο αφορά σε target με έναν μόνο host, είναι έτοιμο! Για να ξεκινήσει αρκεί ένα κλικ στο πράσινο κουμπάκι "play", στα δεξιά της γραμμής.

Παρεμπιπτόντως, αξίζει να αλλάξουμε την τιμή στο λευκό πεδίο που βρίσκεται στην πάνω οριζόντια, πράσινη μπάρα, του Greenbone Security Assistant. Εμείς, π.χ., έχουμε βάλει εκεί την τιμή Refresh every 30 Sec., ώστε κάθε 30 δευτερόλεπτα να ανανεώνονται τα περιεχόμενα της σελίδας κι έτσι να παρακολουθούμε –σχεδόν

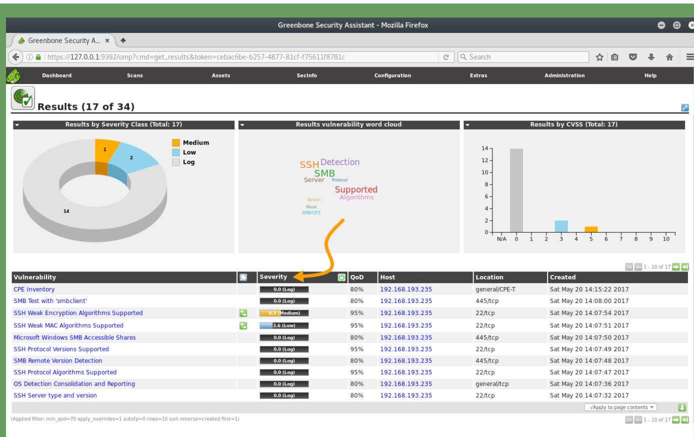
ζωντανά– την πρόοδο του task ή των tasks που έχουμε ξεκινήσει. Όση ώρα διαρκεί το scanning, αν θέλουμε μπορούμε να εξερευνήσουμε άλλες σελίδες του web panel. Το task θα εκτελείται στο background – μάλιστα ακόμη κι αν αποσυνδεθούμε από τον Security Assistant. Για να τσεκάρουμε αν έχει ολοκληρωθεί η διαδικασία ή πώς προχωρά, τέλος πάντων, επιλέγουμε Scans / Tasks. Όταν το scanning τελειώνει, στη στήλη Status και στη γραμμή του αντίστοιχου task βλέπουμε μια γαλάζια μπάρα που γράφει Done. Με κλικ πάνω της εμφανίζονται τα αποτελέσματα του task. Δείτε τα screenshots που ακολουθούν, διαβάστε και τις αντίστοιχες περιγραφές.



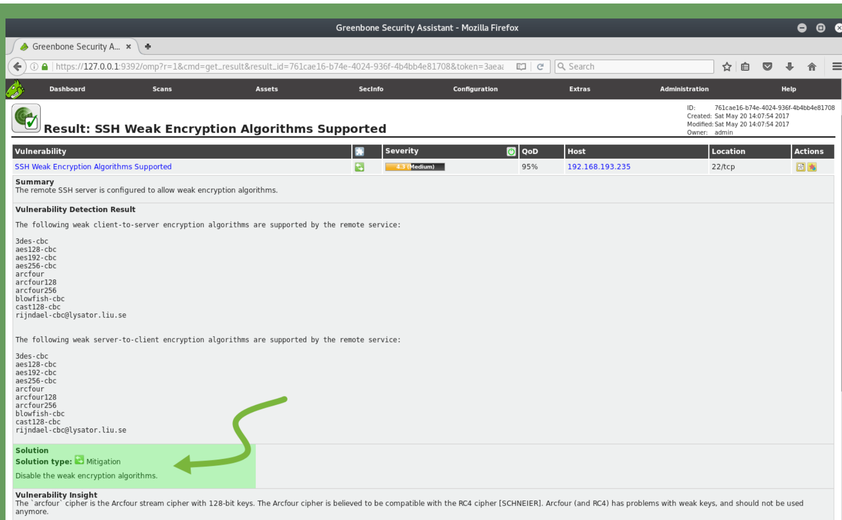
Ο έλεγχος του olafsvik.colder.is για αδυναμίες ολοκληρώθηκε. Στη στήλη Severity το score είναι 4.3, γεγονός που μας προϊδεάζει για κάποια ζητήματα ασφαλείας. Τα αποτελέσματα του ελέγχου τα βλέπουμε με ένα κλικ πάνω στο Done, στη στήλη Status.



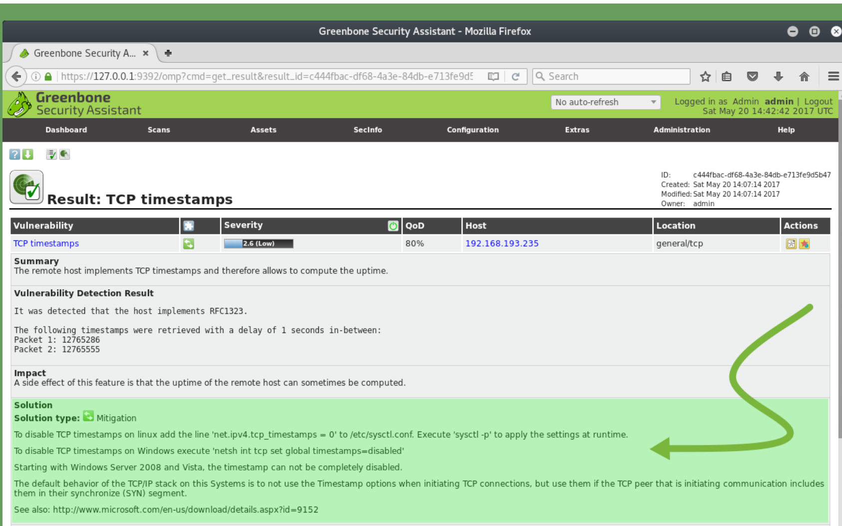
Ιδού η σύντομη λίστα με τα προβλήματα ασφαλείας που αφορούν στο olafsvik. Το σοβαρότερο απ' όλα αφορά στην υπηρεσία SSH και συγκεκριμένα στους χρησιμοποιούμενους αλγόριθμους κρυπτογράφησης, οι οποίοι θα μπορούσαν να είναι ισχυρότεροι.



Αν θέλουμε όλα τα αποτελέσματα ενός task, ακόμη και τα πληροφοριακά μηνύματα που απλά καταγράφονται στο log, τότε επιλέγουμε Scans / Reports και κάνουμε κλικ στο όνομα του task. Στη νέα σελίδα που εμφανίζεται πατάμε πάνω στον αριθμό στα δεξιά της γραμμής Results. Παρατηρήστε ότι τα αποτελέσματα μπορούμε να τα ταξινομούμε με βάση το Severity. Χρήσιμα είναι και τα γραφήματα στο πάνω μέρος της σελίδας, καθώς και το word cloud. Πράγματι, με μια ματιά βλέπουμε πόσο κρίσιμη είναι η κατάσταση, καθώς και σε τι αφορούν τα όποια προβλήματα έχουν εντοπιστεί.



Με κλικ σε μια οποιαδήποτε καταχώρηση της στήλης Vulnerability φορτώνει μια νέα σελίδα, με πολλές περισσότερες πληροφορίες για την αντίστοιχη αδυναμία καθώς και με προτάσεις για την αντιμετώπισή της. Στο screenshot βλέπουμε τους αδύναμους αλγορίθμους κρυπτογράφησης που υποστηρίζει ο SSH server του στόχου, καθώς κι έναν –προφανή, για τη συγκεκριμένη περίπτωση– τρόπο αντιμετώπισης του προβλήματος.



Ιδού κι ένα παράδειγμα αδυναμίας χαμηλού ρίσκου, η οποία αφορά στα λεγόμενα TCP timestamps. Εξαιτίας τους είναι δυνατόν να υπολογιστεί ο χρόνος κατά τον οποίο ο στόχος είναι ενεργός (uptime). Σε κάποια σενάρια δεν θέλουμε να συνάγεται αυτή η πληροφορία, οπότε η λύση είναι να απενεργοποιήσουμε τα TCP timestamps. Στο πλαίσιο Solution περιγράφεται το τι πρέπει να κάνουμε αν το μηχάνημα τρέχει Linux ή Windows.

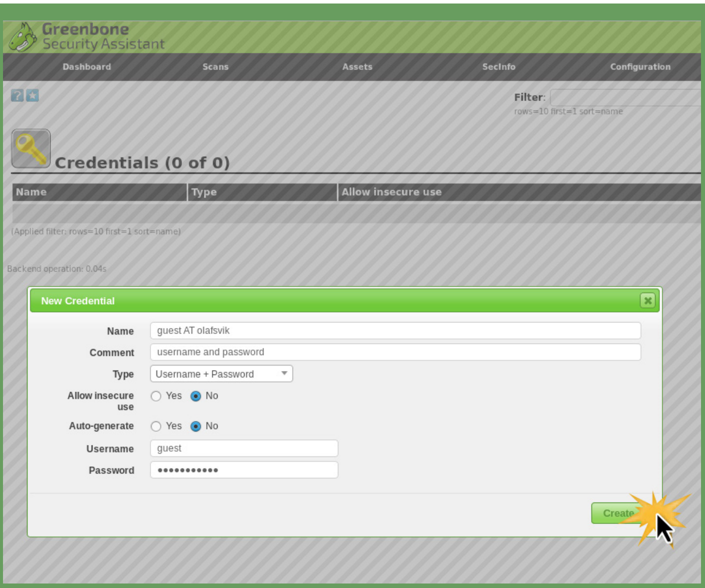
Είναι τα πράγματα χειρότερα απ' όσο δείχνουν;

Στην πραγματική ζωή συχνά είναι, άρα ίσως να 'ναι και στο τεχνολογικό σύμπαν. Μπορεί βέβαια να κάνουμε λάθος, αλλά γιατί ν' αναρωτιόμαστε; Προτείνουμε να δοκιμάσουμε και μετά ο καθένας ας βγάλει τα δικά του συμπεράσματα. Στη συγκεκριμένη περίπτωση, λοιπόν, λέμε να σκανάρουμε ξανά το olafsvik.colder.is για αδυναμίες, αυτή τη φορά όμως με τη γνώση των credentials ενός *απλού* χρήστη του συστήματος, χωρίς δικαιώματα root. Για το παράδειγμα που εξετάζουμε, στο σύστημα-στόχο υπάρχει ένας λογαριασμός απλού χρήστη με username το guest και password το supersecret. Ο χρήστης αυτός έχει απομακρυσμένη πρόσβαση στο μηχάνημα μέσω SSH, αλλά και το δικαίωμα να στέλνει και να παίρνει αρχεία μέσω της SAMBA. Σε κάθε περίπτωση, στην αντίστοιχη υπηρεσία συνδέεται με τα credentials που μόλις παραθέσαμε.

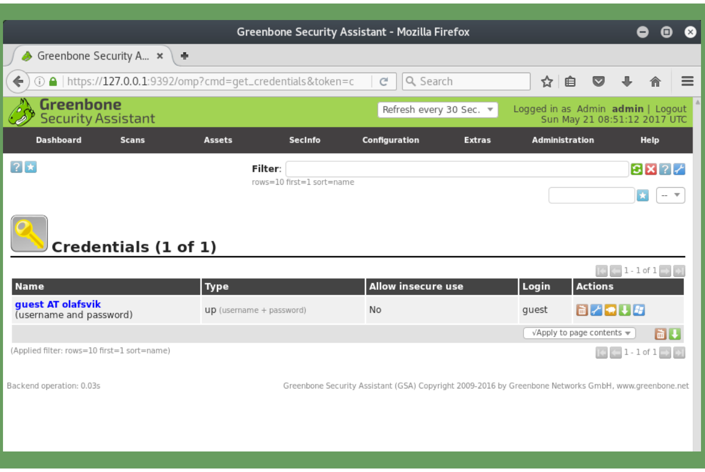
Τώρα, στο OpenVAS έχουμε τη δυνατότητα να δημιουργούμε credentials της μορφής username/password κι ένα ή περισσότερα από αυτά τα ζεύγη να τα αντιστοιχίζουμε σε έναν ή σε περισσότερους στόχους. Μετά φτιάχνουμε αντίστοιχα tasks τα οποία και τρέχουμε, πραγματοποιώντας security scans κατά τα οποία επιτυγχάνονται συνδέσεις σε user accounts των στόχων. Κατ' αυτόν τον τρόπο το OpenVAS συλλέγει πολλές περισσότερες πληροφορίες για λειτουργικά συστήματα και υπηρεσίες, έτσι

τα reports που παράγει είναι πολύ περισσότερο αναλυτικά. Για να δούμε, λοιπόν, τι περισσότερο θα μπορέσουμε –αν μπορέσουμε– να βρούμε για το olafsvik, το στόχο του παραδείγματός μας. Εργαζόμαστε ως ακολούθως.

- Από το web panel του OpenVAS επιλέγουμε Configuration / Credentials.
- Στη σελίδα που εμφανίζεται κάνουμε κλικ στο γαλάζιο κουτάκι με τον αστερίσκο, πάνω αριστερά (New Credential).
- Στο νέο παράθυρο που παρουσιάζεται δίνουμε το username (guest) και το password (supersecret) του χρήστη στο olafsvik.

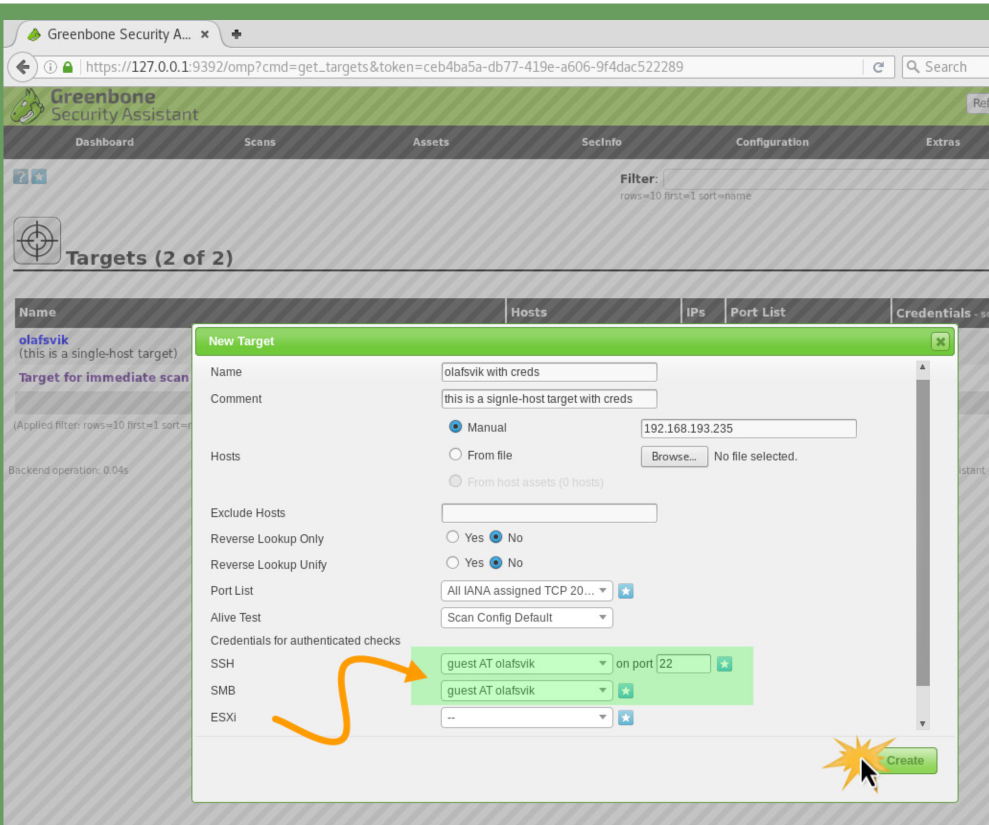


Ορισμός των credentials, δηλαδή του username και του password, του χρήστη guest στο μηχάνημα-στόχο.

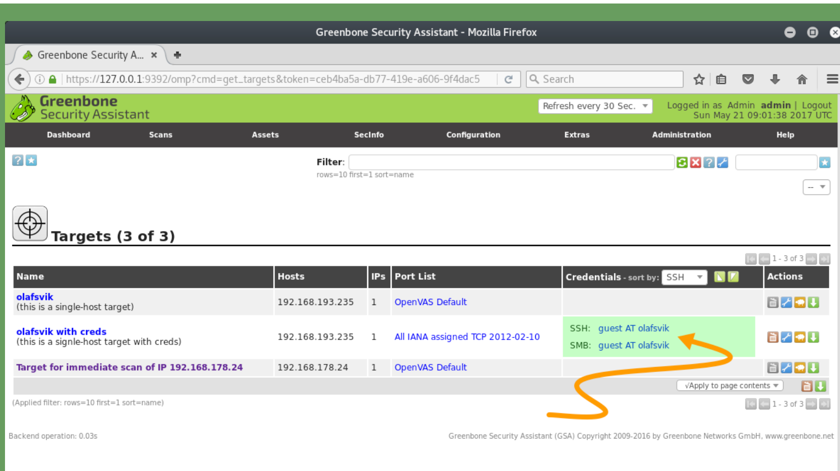


Ιδού τα credentials που έως τώρα γνωρίζει το OpenVAS.

- Πάντα στο web panel του OpenVAS, δίνουμε Configuration / Targets.
- Για άλλη μια φορά πατάμε στο γαλάζιο κουτάκι με τον αστερίσκο, πάνω αριστερά (New Target).
- Στο παράθυρο που εμφανίζεται ορίζουμε, κατά τα γνωστά, νέο στόχο που περιλαμβάνει ένα μόνο μηχάνημα, με IP αυτό του olafsvik. Δεν ξεχνάμε να υποδείξουμε τα credentials για τις συνδέσεις SSH και SMB (SAMBA). Ειδικά για το SSH παρατηρήστε ότι υπάρχει το προκαθορισμένο port, δηλαδή το 22. Αν στο συγκεκριμένο στόχο η υπηρεσία του OpenSSH ακούει από άλλο port, το καθορίζουμε εδώ.

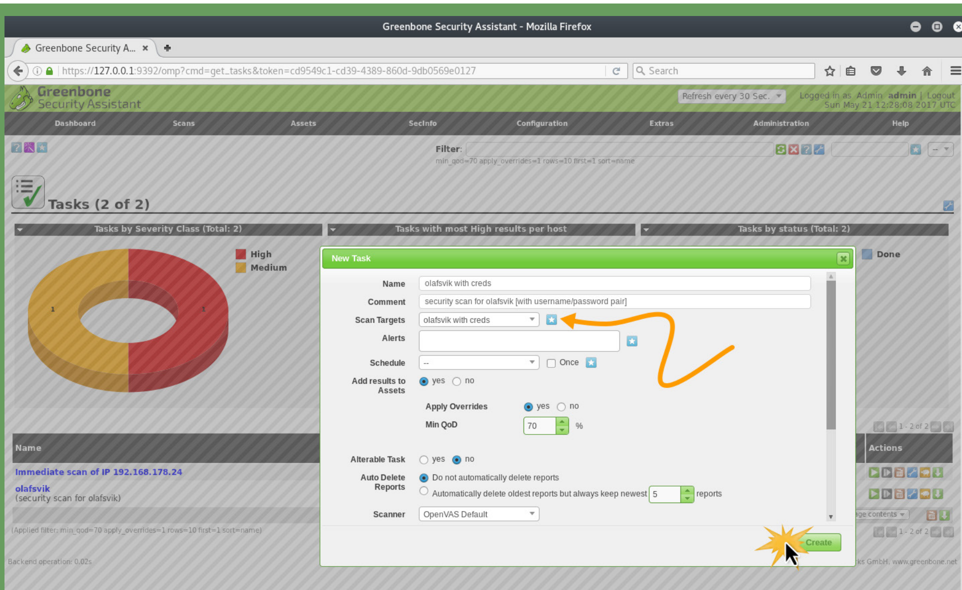


Ορισμός νέου target που περιλαμβάνει ένα μόνο μηχάνημα (με IP το 192.168.193.235), καθώς και τα credentials ενός (απλού) χρήστη του συστήματος-στόχου. Τα στοιχεία σύνδεσης είναι ίδια τόσο για συνδέσεις SSH, όσο και για συνδέσεις μέσω SMB (Samba).

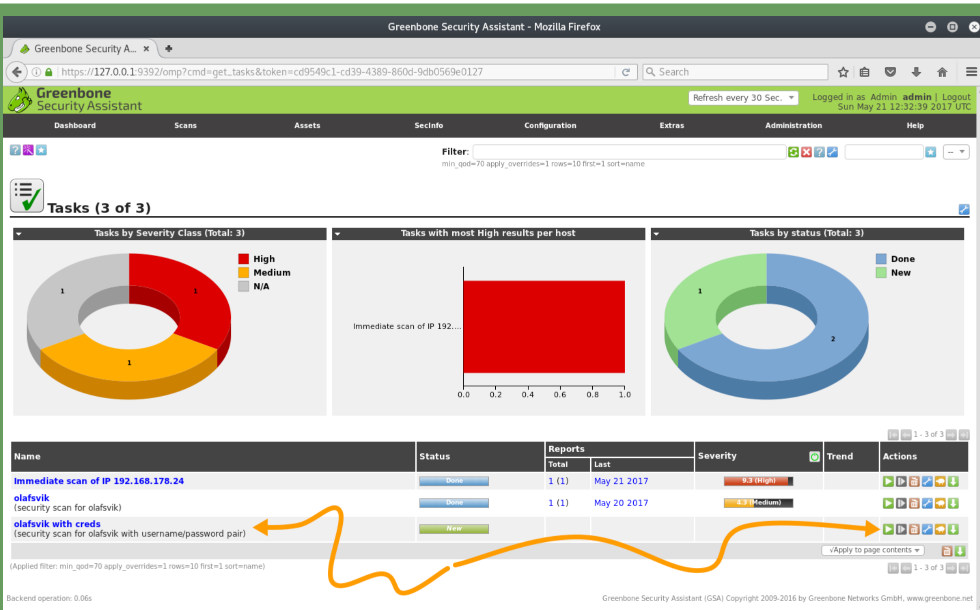


Οι στόχοι που έχουμε ορίσει έως τώρα. Δείτε, παρεμπιπτόντως, εκείνον με το μηχάνημα που έχει IP το 192.168.178.24, το οποίο βρίσκεται σε άλλο τοπικό δίκτυο και τρέχει Windows 7. Στο προκείμενο, παρατηρήστε ότι για το νέο στόχο του olafsvik υπάρχουν πλέον και τα credentials για συνδέσεις στις υπηρεσίες SSH και SMB.

Μένει τώρα να ορίσουμε ένα καινούργιο task, το οποίο θα αφορά στο στόχο που μόλις δημιουργήσαμε. Δίνουμε Scans / Tasks, πατάμε στο γαλάζιο κουμπάκι με τον αστερίσκο και φτιάχνουμε το νέο μας task κατά τα γνωστά.

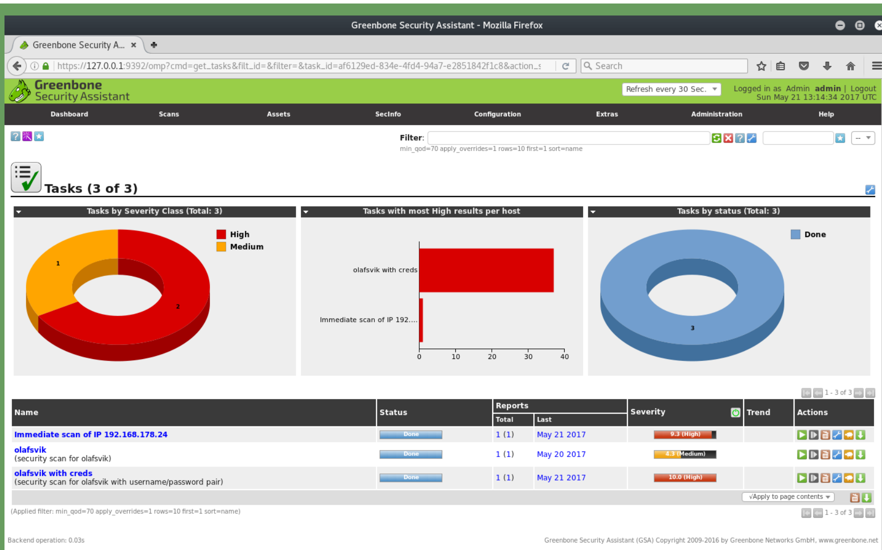


Κατά τη δημιουργία νέου task φροντίζουμε ώστε να υποδείξουμε το target με τα credentials, δηλαδή αυτό που καθορίσαμε πριν λίγο.

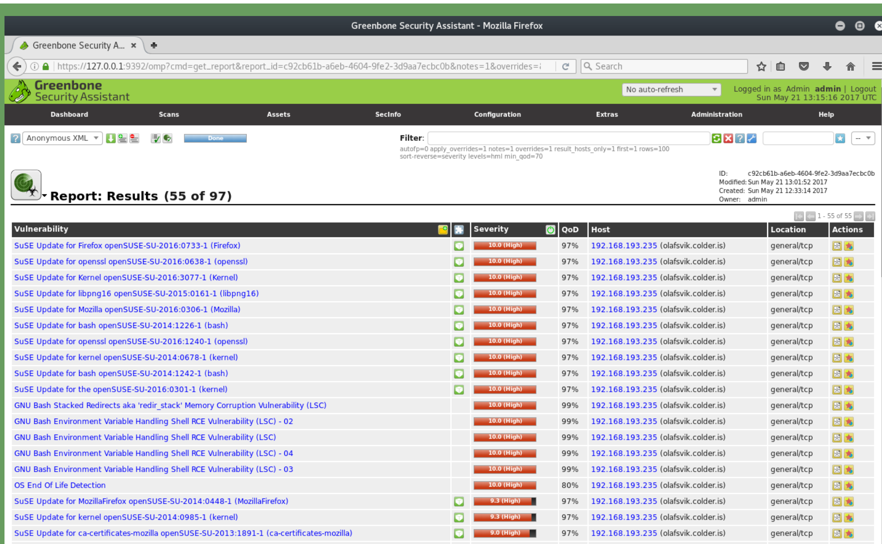


Το νέο task είναι έτοιμο και μπορούμε να το τρέξουμε (κλικ στο πράσινο τετραγωνάκι με το σύμβολο του "play"). Σίγουρα εξάλλου θα προσέξατε το υψηλό Severity εκείνου του άλλου task, για το μηχάνημα με τα Windows 7. Δεν φαίνεται εδώ, σας λέμε όμως ότι η υπηρεσία διαμοίρασης αρχείων ανέβασε τόσο πολύ το score. Το σύστημα είναι για αρκετό καιρό χωρίς ενημερώσεις ασφαλείας κι αυτή τη στιγμή εμφανίζεται ευπαθές ως προς πολύ συγκεκριμένα είδη επιθέσεων.

Το νέο task για το scanning του olafsvik.colder.is –με γνωστά τα credentials για σύνδεση στις υπηρεσίες SSH και SMB– θα χρειαστεί αρκετό πριν ολοκληρωθεί. Μετά το πέρας της διαδικασίας διαπιστώνουμε ότι το Severity score του olafsvik είναι 10, δηλαδή μεγαλύτερο ακόμη κι από το πολύ υψηλό Severity που έχει το unpatched σύστημα με τα Windows 7. Δείτε περισσότερα στα δύο screenshots που ακολουθούν, διαβάστε και τις αντίστοιχες περιγραφές. Επίσης: Πειραματιστείτε και χαρείτε το OpenVAS, τον νέο σας αγαπημένο vulnerability scanner.



Το δεύτερο vulnerability scanning του olafsvik έχει ολοκληρωθεί. Αυτή τη φορά γνωρίζαμε τα credentials ενός απλού χρήστη του συστήματος-στόχου, έτσι το OpenVAS είχε τη δυνατότητα να τρέξει περισσότερα tests (μέσω SSH και SMB). Τα αποτελέσματα δεν χρειάζονται ιδιαίτερο σχολιασμό: έχουμε νέο πρωταθλητή – δυστυχώς με την κακή έννοια :/



Μεταξύ των προβλημάτων ασφαλείας που εντόπισε το OpenVAS στο υπό εξέταση σύστημα, συγκαταλέγονται αδυναμίες στον πυρήνα (kernel), στο BASH shell, στη βιβλιοθήκη glibc, στο bind αλλά και στην υπηρεσία του NTP. Όρεξη να έχουμε να διαβάζουμε λεπτομέρειες για τα vulnerabilities – αλλά και τρόπους αντιμετώπισής τους.

Skill: Intermediate
Tags: KVM, virtualization

Ενεργοποίηση του nested virtualization για το KVM

Σε κάποιες περιπτώσεις χρειάζεται να τρέχουμε εικονικές μηχανές μέσα σε εικονικές μηχανές. Κάτι τέτοιο ίσως ακούγεται περιττό ή/και άσκοπο, στην πραγματικότητα όμως δεν είναι τίποτε από τα δύο.

Υποθέστε, για παράδειγμα, ότι πειραματιζόμαστε με ένα virtual Ceph storage cluster. Εντός του εικονικού δικτύου του cluster θέλουμε κι έναν (εικονικό) KVM server, όπου ορισμένα VMs θα έχουν ως δίσκους block devices που κατοικούν στο storage cluster. Άλλο σενάριο: Εντός ενός VM διερευνούμε τις δυνατότητες του Kubernetes, και μέσα στο VM θέλουμε δύο ή περισσότερα άλλα VMs για να οργανώνει ο Kubernetes τα pods του. Μπορούμε να παραθέσουμε κι άλλα παραδείγματα, νομίζουμε όμως ότι δεν χρειάζεται.

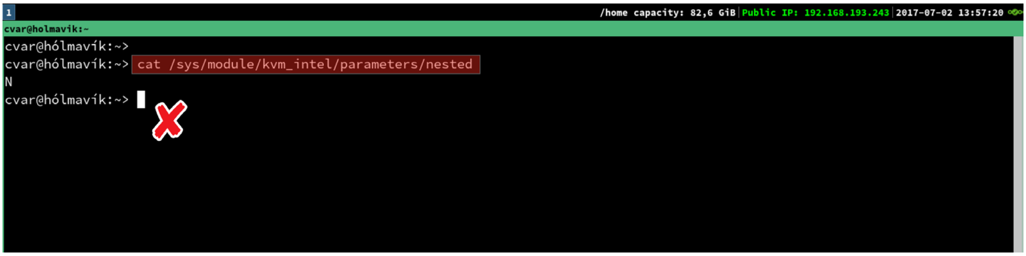
Οι σύγχρονοι hypervizors επιτρέπουν τη δημιουργία εικονικών μηχανών μέσα σε εικονικές μηχανές, κι ο συνδυασμός Linux kernel/KVM δεν αποτελεί εξαίρεση. Πιο συγκεκριμένα, το λεγόμενο *nested virtualization* κάνει δυνατή την εκτέλεση KVM VMs μέσα σε KVM VMs με __ταυτόχρονη__ εκμετάλλευση του hardware acceleration που παρέχει το host computer (physical hardware). Σε έναν οποιονδήποτε Linux host η υποστήριξη nested virtualization ίσως είναι ενεργοποιημένη – αλλά ίσως και όχι. Προκειμένου να δούμε τι ισχύει με τον υπολογιστή μας, από ένα τερματικό πληκτρολογούμε

```
cat /sys/module/kvm_intel/parameters/nested
```

(αν έχουμε Intel CPU) ή

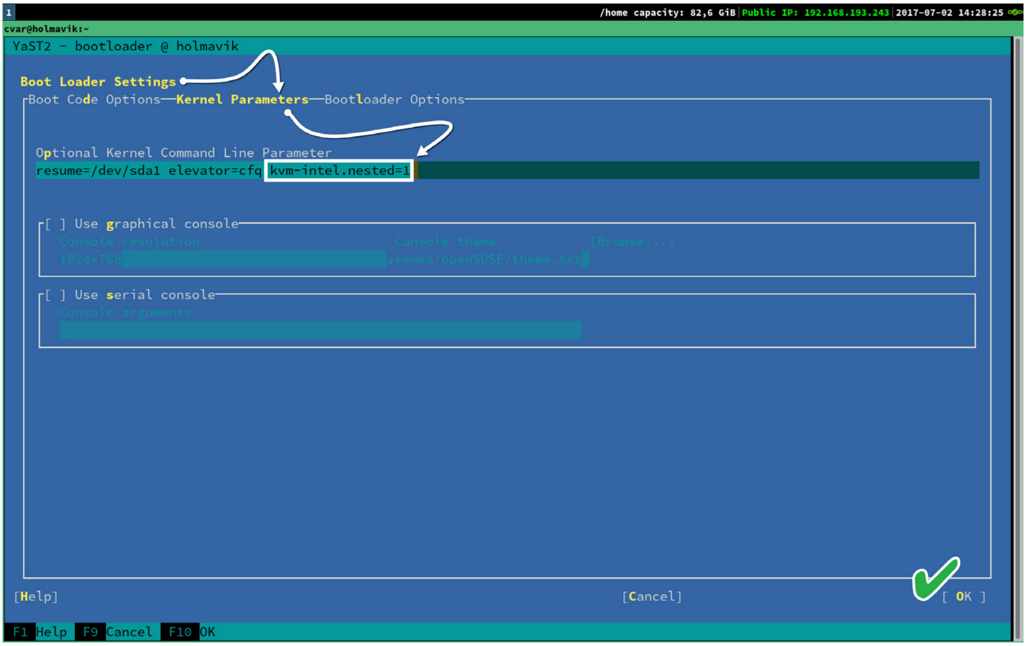
```
cat /sys/module/kvm_amd/parameters/nested
```

(αν έχουμε AMD CPU). Στην περίπτωση που το cat επιστρέψει 0 ή N, τότε το nested virtualization είναι απενεργοποιημένο. Αν πάλι επιστρέψει 1 ή Y, τότε το nested virtualization είναι ενεργοποιημένο.



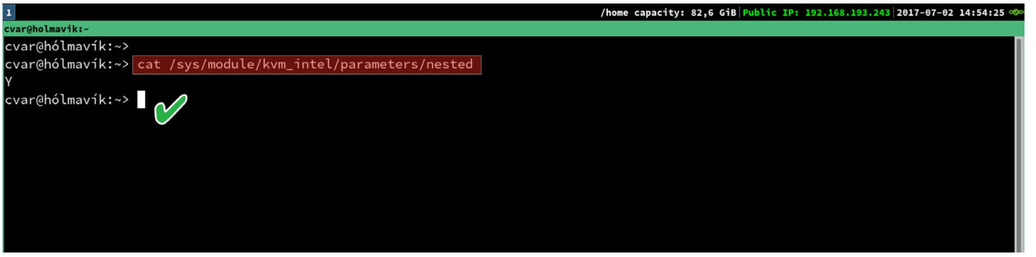
Στον Intel-based Linux host των δοκιμών μας, το nested virtualization ήταν εξ ορισμού απενεργοποιημένο.

Αν ο υπολογιστής σας έχει επεξεργαστή AMD, το nested virtualization πιθανώς είναι ήδη ενεργοποιημένο. Αν από την άλλη έχετε μηχάνημα με επεξεργαστή Intel, τότε το nested virtualization ίσως δεν είναι ενεργοποιημένο. Σε μια τέτοια περίπτωση, αξίζει να δοκιμάσουμε την εκκίνηση του host OS έχοντας δώσει στον πυρήνα την παράμετρο kvm-intel.nested=1. Ειδικά στο openSUSE που πολύ αγαπάμε, με τη βοήθεια του YaST module ονόματι bootloader είναι πανεύκολο να ρυθμίσουμε τον GRUB ώστε η προαναφερθείσα παράμετρος να περνάει __πάντοτε__ στον πυρήνα κατά το boot.



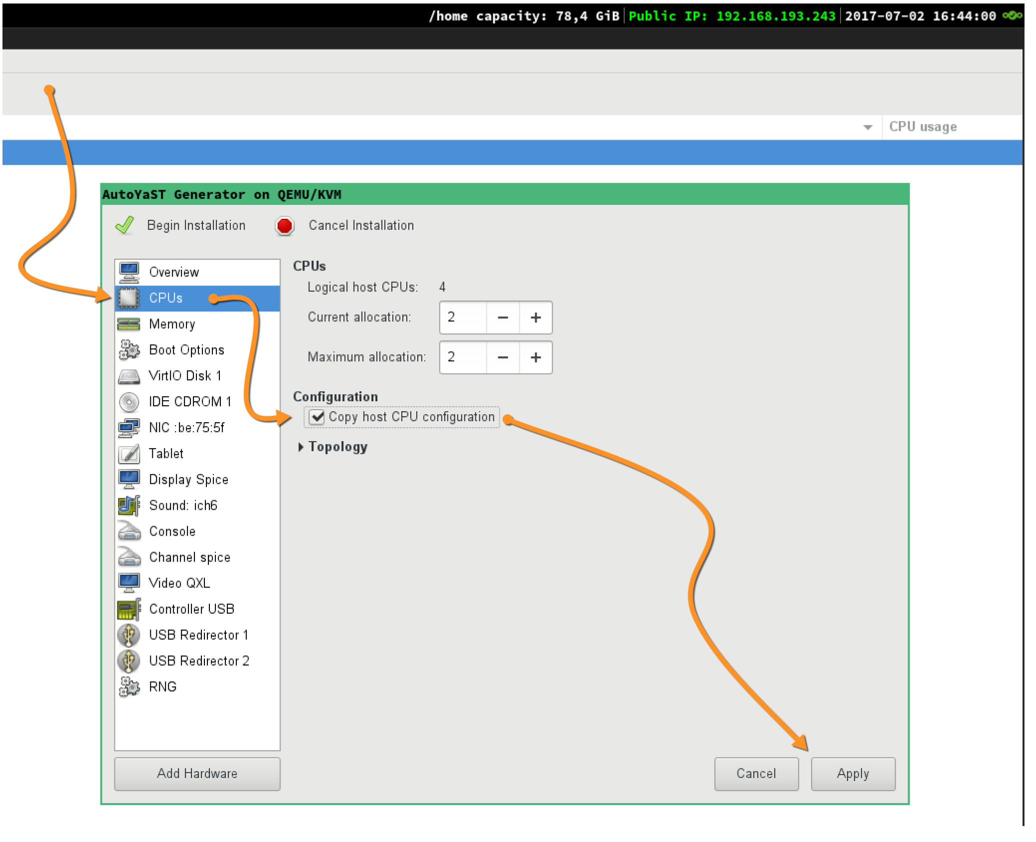
Χρήση του YaST module ονόματι bootloader, ώστε να τροποποιήσουμε τις παραμέτρους που περνούν στον πυρήνα κατά το boot.

Η νέα παράμετρος για τον πυρήνα λαμβάνεται υπόψη μετά την επόμενη επανεκκίνηση του λειτουργικού. Ξανά από ένα τερματικό, πληκτρολογούμε και πάλι cat /sys/module/kvm_intel/parameters/nested κι ελέγχουμε το αποτέλεσμα. Αν και τώρα δεν δούμε 1 ή Y, τότε είτε ο επεξεργαστής είτε ο πυρήνας του λειτουργικού είναι αρκετά παλιός.



Μετά την επανεκκίνηση του λειτουργικού κι έχοντας περάσει στον Linux kernel την κατάλληλη παράμετρο, με χαρά διαπιστώνουμε ότι το nested virtualization υποστηρίζεται από το σύστημά μας.

Με το nested virtualization ενεργοποιημένο είμαστε πλέον σε θέση να φτιάχνουμε VMs μέσα σε VMs, όπου τα nested VMs θα εκμεταλλεύονται το hardware acceleration του physical host. Οφείλουμε όμως να φροντίζουμε ώστε, για τα VMs που θα αποτελούν hosts άλλων VMs, να ισχύει συγκεκριμένη ρύθμιση όσον αφορά στον εικονικό τους επεξεργαστή. Δείτε το screenshot που ακολουθεί, όπου διακρίνεται η σχετική ρύθμιση στο περιβάλλον του virt-manager.

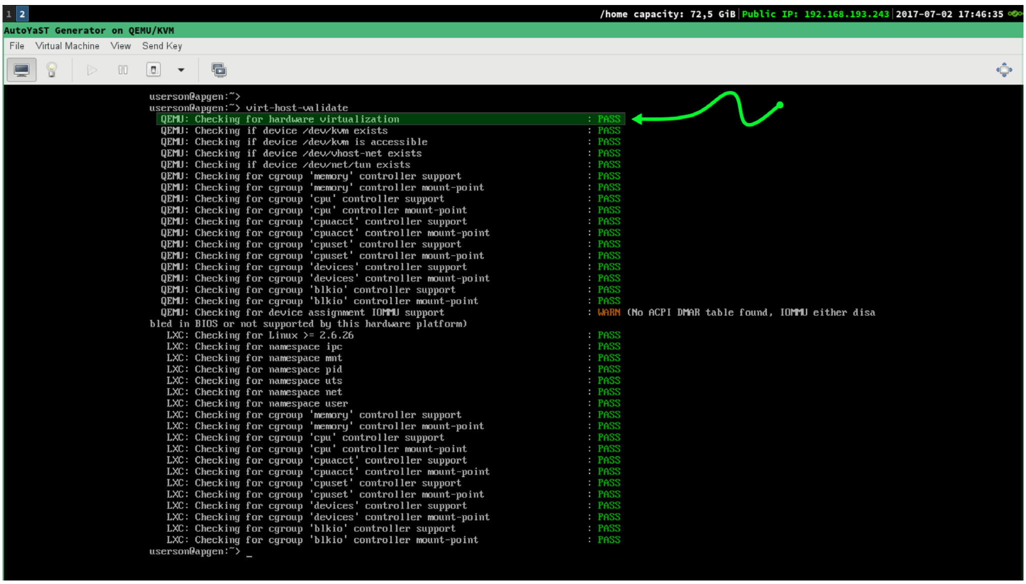


Το συγκεκριμένο VM θα αποτελέσει τον host άλλων VMs. Γι' αυτό και μέσα από το περιβάλλον του virt-manager φροντίζουμε ώστε για τη CPU του VM να είναι τσεκαρισμένο το Copy host CPU configuration.

Για ένα KVM VM που θα αποτελέσει τον host άλλων KVM VMs, μένει ένας τελευταίος έλεγχος που καλό είναι να κάνουμε __μέσα__ από το guest OS του virtualized host. Συγκεκριμένα, αρκεί να πληκτρολογήσουμε

```
virt-host-validate
```

και να παρατηρήσουμε το αποτέλεσμα του ελέγχου περί hardware virtualization (στο openSUSE, το εργαλείο βρίσκεται στο πακέτο libvirt-client).



Αυτό το VM θα αποτελέσει τον host άλλων VMs, τα οποία θα εκμεταλλεύονται το hardware acceleration του physical host. Το αποτέλεσμα του πρώτου ελέγχου που διενεργεί το virt-host-validate επιβεβαιώνει ότι, πράγματι, έτσι θα συμβαίνει.

Όπως φαίνεται και στο screenshot, το αποτέλεσμα θα πρέπει να είναι "PASS".

ΥΓ. Φτιάξτε τον δικό σας __physical__ KVM server χωρίς ιδιαίτερα ισχυρό hardware. Διαβάστε περισσότερα στη σχετική σειρά άρθρων: https://deltahacker.gr/osuse-virt-host-p1.

Skill: Intermediate
Tags: WannaCry, SambaCry, Samba, SMB, Kali Linux, Metasploit

Το WannaCry του Linux και η εκμετάλλευσή του

Η πρόσφατη ιστορία με το WannaCry, το ransomware που ταχύτατα μόλυνε εκατοντάδες χιλιάδες υπολογιστές Windows σε όλο τον πλανήτη, θύμισε σε πολλούς πόσο σημαντικό είναι να διατηρούμε το λειτουργικό μας σύστημα ενημερωμένο. Αλλά ευπαθή δεν αποδεικνύονται μόνο τα μηχανήματα με Windows.

Λίγο η αναβλητικότητα των διαχειριστών, λίγο η νοοτροπία του "αυτά συμβαίνουν σε άλλους", και το αποτέλεσμα είναι πως για άλλη μια φορά ένα Windows malware βρήκε πρόσφορο έδαφος κι εξαπλώθηκε ταχύτατα σε όλο τον πλανήτη. Κάποιος θα προσέθετε –και θα είχε 100% δίκιο– ότι υπάρχουν δύο ακόμα λόγοι για τη διάδοση κακόβουλου λογισμικού όπως το WannaCry ή WannaCrypt, όπως αλλιώς ονομάζεται: α) οι χρήστες Windows είναι ιλιγγιωδώς πολλοί, β) στην πλειονότητά τους έχουν ελλιπείς τεχνικές γνώσεις και άγνοια περί βασικών θεμάτων ασφαλείας. Έτσι, τα συστήματά τους είναι μη-ενημερωμένα ή/και αφελώς ρυθμισμένα – συνεπώς κι ευπαθή.

Στον αντίποδα έχουμε τους χρήστες και τους διαχειριστές συστημάτων Linux. Κατά κύριο λόγο είναι τεχνικά καταρτισμένοι, ενώ γνωρίζουν αρκετά και για το πώς δουλεύουν τα exploits και οι επιθέσεις που τα εκμεταλλεύονται. Την ίδια στιγμή όμως ο πυρήνας του Linux, οι υπηρεσίες, τα προγράμματα στο userland και οι εφαρμογές που προσφέρονται μέσω Internet, εξακολουθούν να αναπτύσσονται και να συντηρούνται από ανθρώπους – και οι άνθρωποι κάνουν λάθη. Όταν λοιπόν ερευνητές ασφαλείας ανακαλύπτουν αδυναμίες που αφορούν, π.χ., σε δημοφιλείς υπηρεσίες που συναντάμε σε διανομές Linux, εκδοχές του BSD κ.ο.κ., καθόλου δεν πρέπει να εκπλησσόμεθα.

Καλωσόρισες SambaCry!

Όπως διαπιστώθηκε λίγες μέρες μετά το ξέσπασμα του WannaCry, τα Windows δεν είναι το μόνο σύστημα με ευπάθεια remote execution μέσω του πρωτοκόλλου SMB (Server Message Block, https://en.wikipedia.org/wiki/Server_Message_Block). Το

ίδιο συμβαίνει και με συστήματα Linux που τρέχουν τη σουίτα διαμοίρασης αρχείων SAMBA. Το σχετικό bug μάλιστα ήταν εκεί για επτά ολόκληρα χρόνια και κανείς δεν το 'χε παρατηρήσει.

Ο λόγος γίνεται για το CVE-2017-7494, μια ευπάθεια απομακρυσμένης εκτέλεσης που υφίσταται στις εκδόσεις της Samba από την 3.5.0 και νεότερες (http://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2017-7494). Το SambaCry, όπως ονομάστηκε το bug, από τεχνικής σκοπιάς είναι εντελώς διαφορετικό από το EternalBlue, ένα από τα bugs που εκμεταλλεύεται το WannaCry (https://en.wikipedia.org/wiki/EternalBlue). Πράγματι, ενώ το EternalBlue αποτελεί ένα buffer overflow exploit, το δε SambaCry αφορά στο αυθαίρετο (μη-εξουσιοδοτημένο) φόρτωμα βιβλιοθηκών. Για την εκμετάλλευση του SambaCry ο επιτιθέμενος αρκεί ν' ανεβάσει μια κατάλληλη βιβλιοθήκη σ' ένα Samba share στο οποίο επιτρέπεται η εγγραφή αρχείων. Σε πολλές εγκαταστάσεις της σουίτας, για την ευκολία των χρηστών υπάρχει τουλάχιστον ένα τέτοιο share. Έχει ρόλο κοινόχρηστου χώρου διαμοίρασης αρχείων, για τους μόνιμους χρήστες του τοπικού δικτύου ή και για τους περιστασιακούς. Η βιβλιοθήκη που ανεβάζει ο επιτιθέμενος στο share, λοιπόν, είναι δυνατό να διαβαστεί από τον Samba server, ο οποίος και θα εκτελέσει τον κώδικα που περιλαμβάνει.

Το CVE-2017-7494 αντιμετωπίστηκε γρήγορα από τους developers της Samba, οπότε ο καλύτερος τρόπος για την προστασία από το bug είναι η αναβάθμιση της σουίτας. Το πρόβλημα είναι σοβαρότερο με τα NAS. Η αναβάθμιση για τέτοια boxes συχνά σημαίνει ότι πρέπει να κατεβάσουμε το κατάλληλο firmware από το site του κατασκευαστή, ο οποίος όμως δεν είναι σίγουρο ότι θα βιαστεί να κυκλοφορήσει νεότερη έκδοση, απαλλαγμένη από το SambaCry. Αν μάλιστα μιλάμε για μοντέλα που πλέον δεν υποστηρίζονται, δεν έχει νόημα να περιμένουμε από τον κατασκευαστή να κάνει μια εξαίρεση και να κυκλοφορήσει update.

Επίδειξη επίθεσης με το Metasploit

Έχει ήδη κυκλοφορήσει ένα exploit module για το Metasploit, το οποίο εκμεταλλεύεται το SambaCry και δουλεύει σε στόχους αρχιτεκτονικής x86, x86-64 και ARM (μην ξεχνάτε τα NAS boxes). Στη συνέχεια του άρθρου εργαζόμαστε από το Kali Linux κι επιδεικνύουμε μια επίθεση που πραγματοποιείται με τη βοήθεια του Metasploit, προς έναν Linux Samba server ο οποίος είναι ευπαθής κατά το CVE-2017-7494. Με την ευκαιρία δείχνουμε και πώς σκανάρουμε hosts εντός του τοπικού δικτύου μέσα από το Metasploit, αλλά και πώς χρησιμοποιούμε τα exploit modules της πλατφόρμας.

Αρχίζουμε ενημερώνοντας το Kali Linux, αν μη τι άλλο επειδή έτσι ίσως αναβαθμιστεί και το Metasploit και συνεπώς θα 'χουμε το exploit module για το CVE-2017-7494:

```
root@kali:~# apt-get update
root@kali:~# apt-get upgrade
```

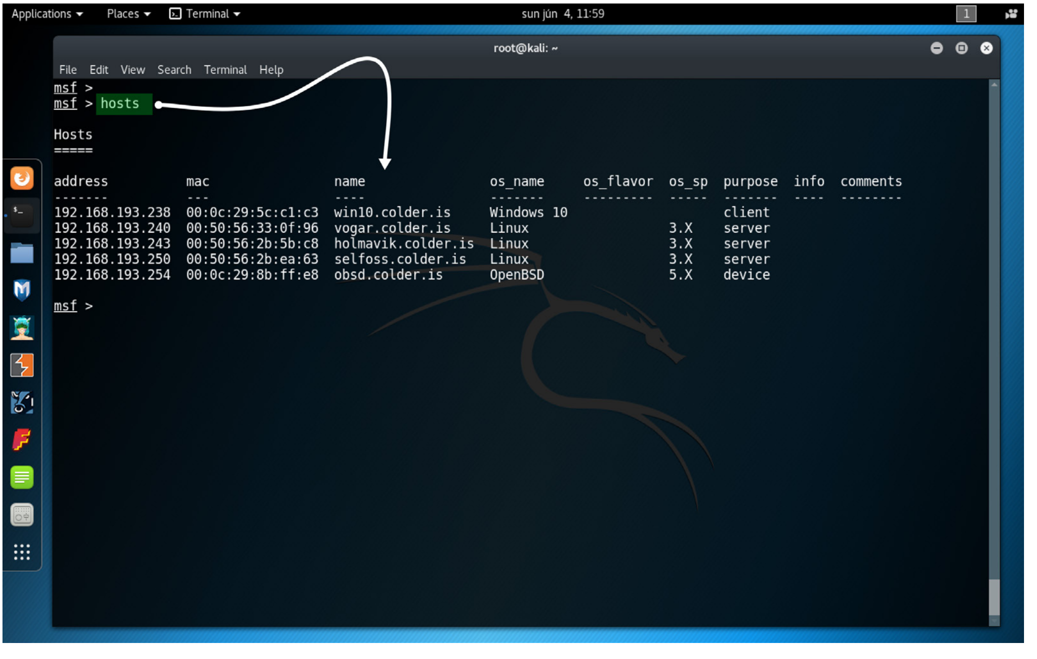
Ξεκινάμε το Metasploit, φροντίζοντας ώστε να επικοινωνεί με την PostgreSQL (https://deltahacker.gr/kali-metasploit-postgresql). Θέλουμε να σκανάρουμε όλα τα μηχανήματα του τοπικού δικτύου και τις σχετικές πληροφορίες να τις αποθηκεύσουμε στη βάση του Metasploit. Στο prompt της πλατφόρμας, πληκτρολογούμε:

```
msf > db_nmap -Pn -sS -sV -O 192.168.193.0/24
```

(Τα μηχανήματα του τοπικού μας δικτύου έχουν διευθύνσεις IP της μορφής 192.168.193.*, εσείς βεβαίως βάλτε τη μορφή των διευθύνσεων για το δικό σας δίκτυο.) Μόλις το scanning ολοκληρωθεί, δίνουμε

```
msf > hosts
```

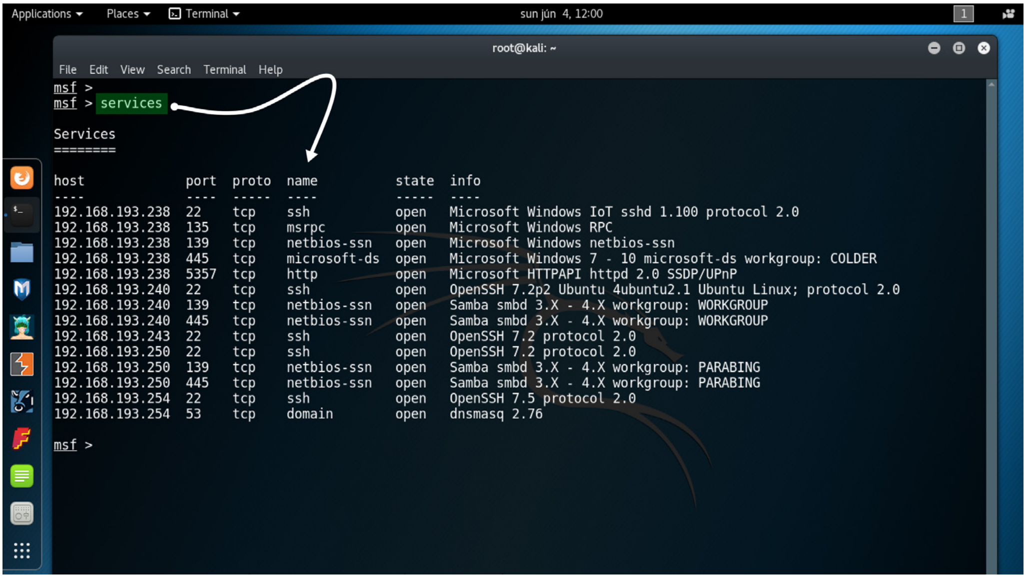
και βλέπουμε τα μηχανήματα που εντοπίστηκαν κι αποθηκεύτηκαν στη βάση του Metasploit.



Τρέξαμε το nmap μέσα από το Metasploit (db_nmap) και τα ενεργά μηχανήματα που βρέθηκαν αποθηκεύτηκαν στη βάση δεδομένων της πλατφόρμας. Πληκτρολογώντας hosts παίρνουμε τη λίστα με όλα αυτά τα hosts.

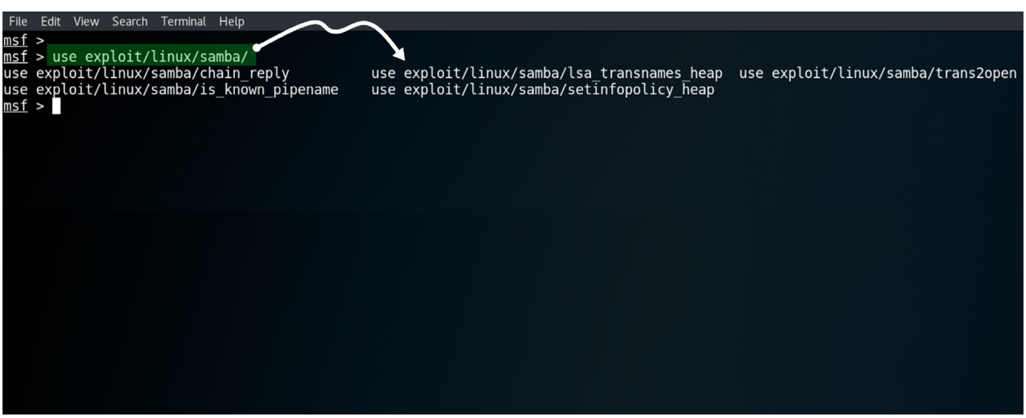
Όλες τις ενεργές υπηρεσίες όλων των hosts που βρήκε το db_nmap, τις βλέπουμε πληκτρολογώντας:

```
msf > services
```



Το db_nmap που μόλις τρέξαμε δεν αποθήκευσε στη βάση του Metasploit μόνο τα hosts που βρήκε, αλλά και τις ενεργές υπηρεσίες που έχουν.

Εξετάζοντας τα έως τώρα αποτελέσματα, εύκολα διαπιστώνουμε ότι έχουμε έναν host με Windows, τρεις με Linux κι έναν με OpenBSD. Δύο από τα Linux hosts έχουν τη Samba ενεργοποιημένη, οπότε θα επικεντρώσουμε την προσοχή μας σε αυτά. Το exploit που ψάχνουμε είναι για Linux και συγκεκριμένα για τη Samba. Αν θέλουμε να δούμε *όλα* τα σχετικά exploits για τη Samba στο Linux, στη γραμμή εντολών του Metasploit γράφουμε use exploit/linux/samba και πατάμε δύο φορές το πλήκτρο [Tab].

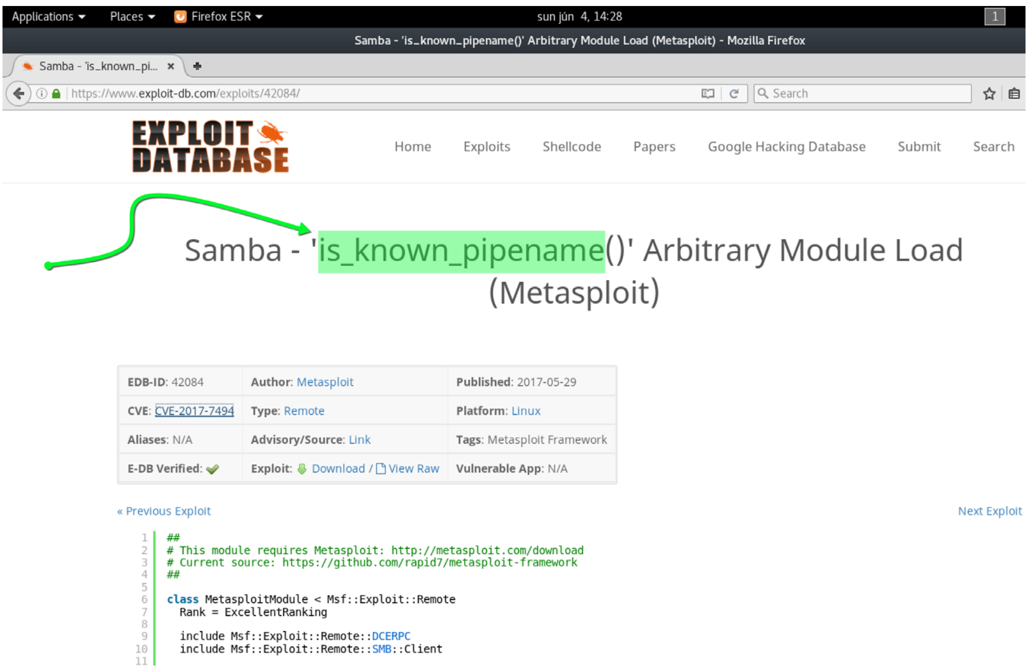


Το Tab completion, όπως το ξέρουμε από το BASH, δουλεύει και στην κονσόλα του Metasploit. Στο εικονιζόμενο παράδειγμα το εφαρμόζουμε ώστε να δούμε όλα τα διαθέσιμα exploits για τη Samba στο Linux.

Υπάρχουν πέντε τέτοια exploits. Προκειμένου να εντοπίσουμε εκείνο που τώρα θέλουμε, πατάμε το συνδυασμό πλήκτρων [CTRL+C] και καταφεύγουμε στην εντολή info. Για παράδειγμα, γράφουμε

```
msf > info exploit/linux/samba/is_known_pipename
```

και διαβάζουμε την περιγραφή για το is_known_pipeline. Εναλλακτικά, από έναν web browser πηγαίνουμε στη διεύθυνση https://www.exploit-db.com/search και κάνουμε μια αναζήτηση για το CVE του exploit – εν προκειμένω για το CVE-2017-7494. Στα αποτελέσματα της αναζήτησης θα δούμε και το όνομα του exploit module.



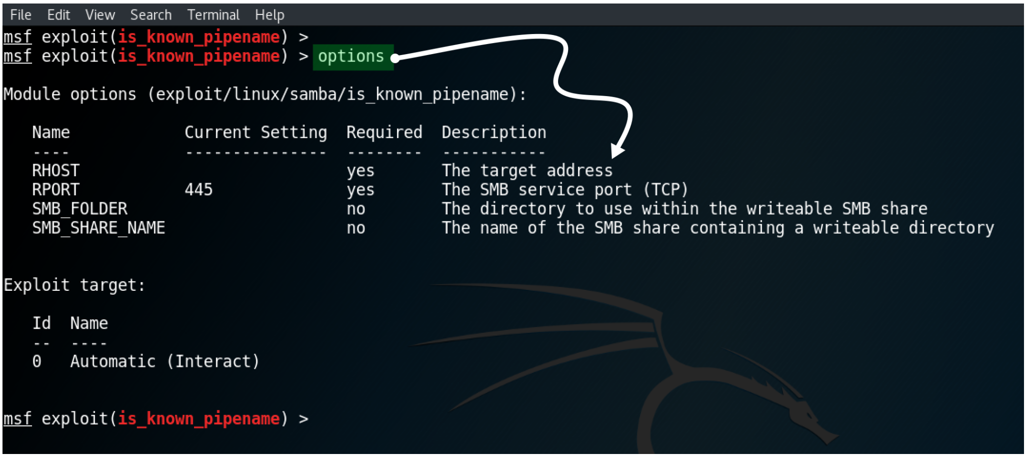
Αναζητήσεις για exploits μπορούμε να κάνουμε κι από το βολικό site της Exploit Database.

Το exploit που ψάχνουμε, λοιπόν, είναι το is_known_pipename. Το φορτώνουμε δίνοντας:

```
msf > use exploit/linux/samba/is_known_pipename
```

Παρατηρήστε ότι το prompt του Metasploit αλλάζει, ώστε να περιλαμβάνει το όνομα του exploit που μόλις φορτώσαμε. Κάθε exploit δέχεται παραμέτρους, τις οποίες βλέπουμε πληκτρολογώντας:

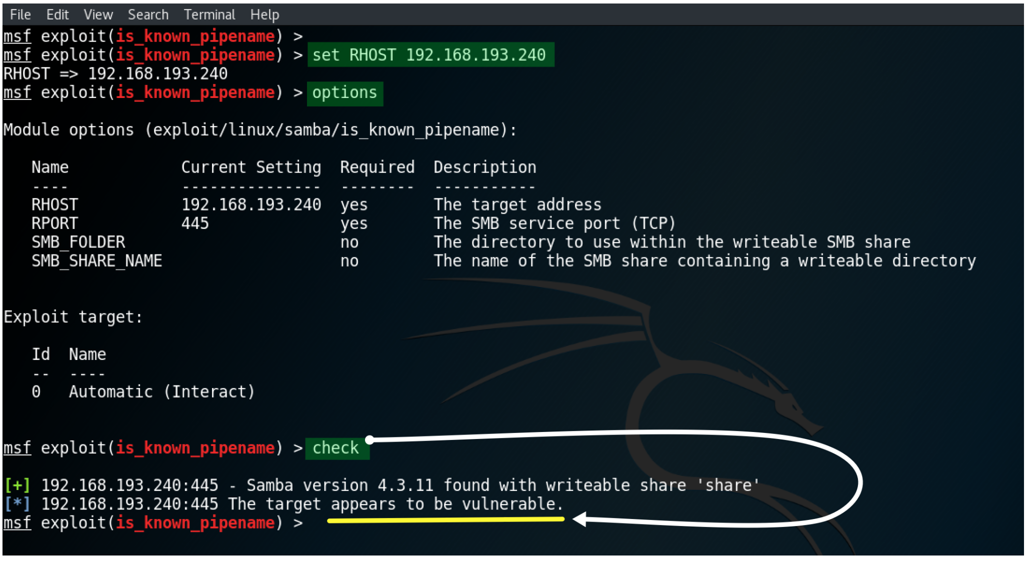
```
msf exploit(is_known_pipename) > options
```



Ιδού οι παράμετροι που δέχεται το exploit για την εκμετάλλευση του SambaCry. Από τις υποχρεωτικές, RHOST και RPORT, χρειάζεται να αναθέσουμε τιμή μόνο στην πρώτη. Αναλυτικότερα, θα τις δώσουμε τη διεύθυνση IP του μηχανήματος-στόχου.

Η RHOST είναι υποχρεωτική κι αποθηκεύει τη διεύθυνση IP του στόχου. Έχουμε δύο υποψήφιους στόχους, με διευθύνσεις IP 192.168.193.240 και 192.168.193.250 (δεν αρκεί μόνο η έξοδος της εντολής hosts, αλλά χρειάζεται και η έξοδος της services). Ας δοκιμάσουμε με το vogar.colder.is (192.168.193.240):

```
msf exploit(is_known_pipename) > set RHOST 192.168.193.240
```



Μετά από έναν απλό έλεγχο, χωρίς να γίνει κάποια προσπάθεια για exploitation, όλα δείχνουν ότι ο στόχος μας είναι ευπαθής ως προς το CVE-2017-7494 – ή αλλιώς SambaCry.

Επαληθεύουμε ότι η ανάθεση τιμής στην RHOST πέτυχε, δίνοντας:

```
msf exploit(is_known_pipename) > options
```

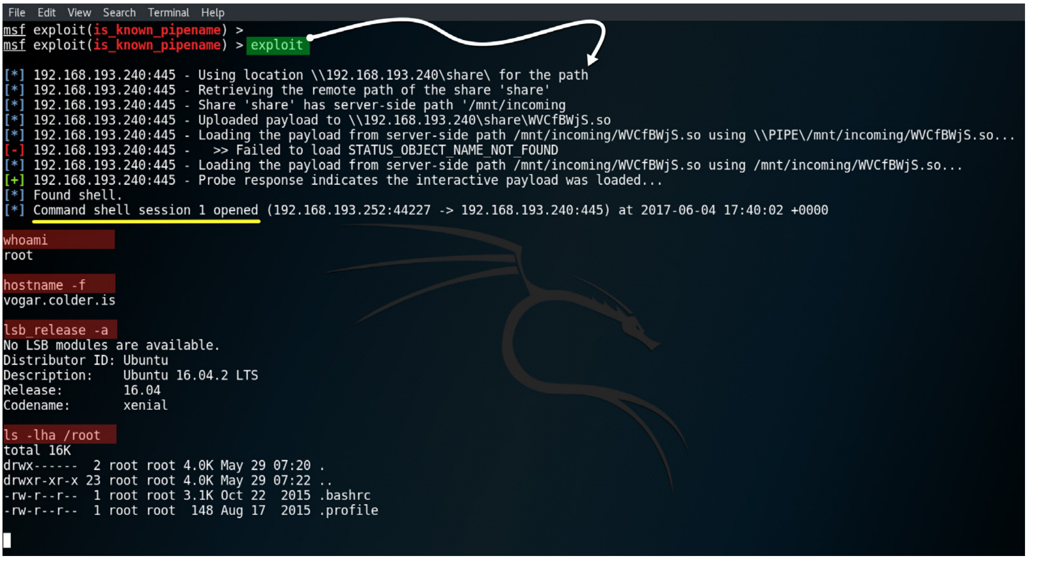
Είναι ο στόχος, με IP αυτό που έχουμε αναθέσει στην παράμετρο RHOST, πράγματι ευπαθής ως προς το CVE-2017-7494; Πριν καν επιχειρήσουμε να εξαπολύσουμε μια επίθεση, μπορούμε να κάνουμε έναν απλό έλεγχο με την εντολή check του Metasploit:

```
msf exploit(is_known_pipename) > check
```

Ωραία, ο στόχος μοιάζει να είναι πράγματι ευπαθής. Προκειμένου να εξαπολύσουμε την επίθεσή μας, αρκεί να γράψουμε:

```
msf exploit(is_known_pipename) > exploit
```

Δείτε τα αποτελέσματα στο screenshot που ακολουθεί, διαβάστε και τη σχετική περιγραφή.



Η εκμετάλλευση του exploit για το SambaCry ήταν επιτυχής! Αν και στο τερματικό δεν απεικονίζεται κάποιο σχετικό prompt, το μήνυμα "Command shell session 1 opened" φανερώνει ότι έχουμε shell access στον απομακρυσμένο host. Πληκτρολογώντας μερικές εντολές (βλέπε εκείνες στο κόκκινο υπόβαθρο) βεβαιωνόμαστε ότι πράγματι κινούμαστε εντός του μηχανήματος-στόχου, έχοντας μάλιστα πρόσβαση στο λογαριασμό του ίδιου του root!


CMYK & WEB
cmykandweb.gr
GRAPHIC DESIGN
design • layout • web

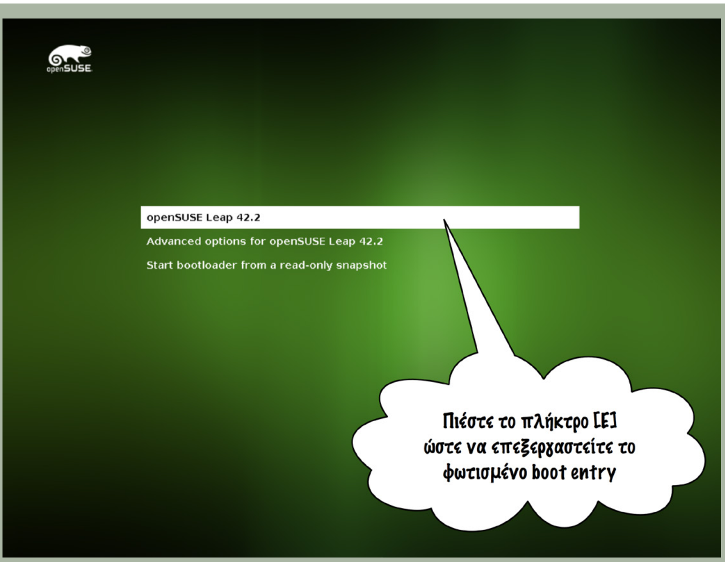
Skill: Beginner
Tags: openSUSE, Fedora, Ubuntu, GRUB2, local access hacks

Πώς επανακαθορίζουμε ξεχασμένο root password στο Linux

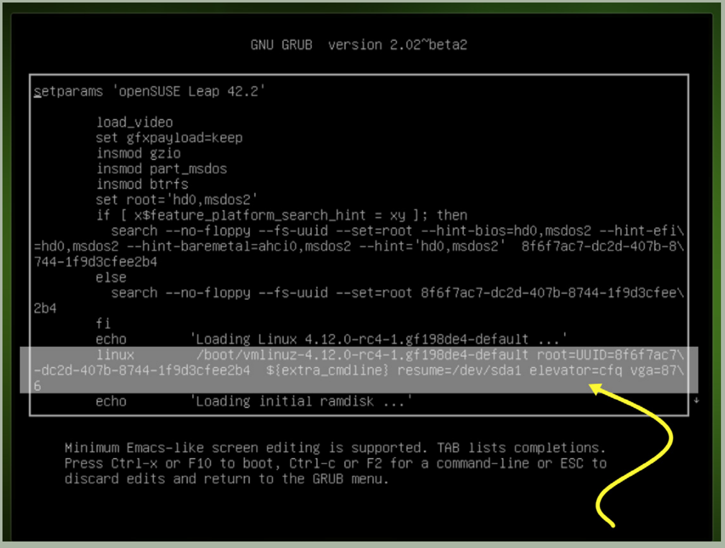
Πότε ήταν η τελευταία φορά που με τρόμο συνειδητοποιήσατε ότι δεν θυμόσαστε το root password σε υπολογιστή με Linux; Όσο άσχετο κι αν σας φαίνεται το ερώτημα (ή όσο κι αν ντρεπόσαστε να παραδεχτείτε ότι την έχετε ήδη πάθει), ας σημειώσουμε ότι το να ξεχάσει κάποιος το συνθηματικό του διαχειριστή δεν είναι κάτι που συμβαίνει σπάνια.

Την επόμενη φορά που δεν θα μπορείτε να συνδεθείτε στο root account κάποιου υπολογιστή σας με Linux, μην πανικοβληθείτε. Πάρτε μια βαθιά ανάσα κι αναρωτηθείτε: Υπάρχει μήπως άλλος υπολογιστής ή συσκευή, απ' όπου έχετε φροντίσει για passwordless SSH logins στον υπό συζήτηση λογαριασμό; (https://deltahacker.gr/?p=13357) Αν ναι, απλά πηγαίνετε σ' αυτόν τον άλλον υπολογιστή ή συσκευή, συνδεθείτε στο προαναφερθέν root account απομακρυσμένα, αλλάξτε το password με το εργαλείο passwd, αγαλιάστε και χαρείτε. Ίσως όμως να μην έχετε φροντίσει για passwordless logins – τουλάχιστον όχι σε root accounts. Ή μπορεί να 'χετε φροντίσει, αλλά τώρα δεν έχετε εύκαιρο τον άλλον υπολογιστή ή συσκευή. Σε κάθε περίπτωση, αν έχετε φυσική πρόσβαση στον υπολογιστή με το ξεχασμένο root password, κι αυτός με τη σειρά του διαθέτει ένα ταπεινό πληκτρολόγιο και μια σεμνή οθόνη, μάθετε ότι είναι εύκολο να ορίσετε καινούργιο password για τον root – κι ας μη θυμόσαστε το παλιό.

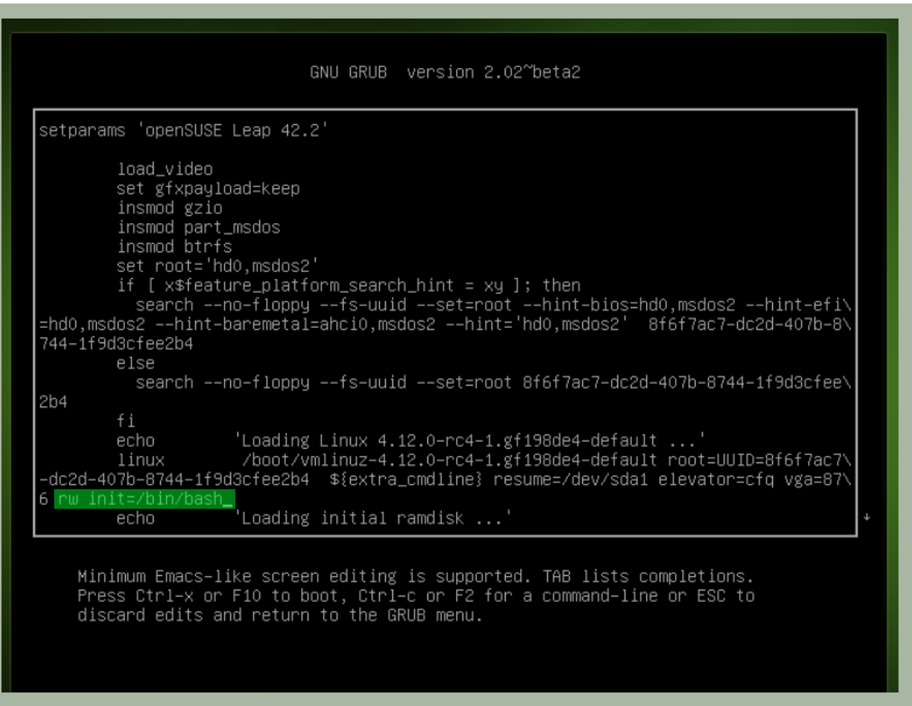
Στη συνέχεια δείχνουμε πώς αλλάζουμε το ξεχασμένο root password συστήματος με openSUSE Leap 42.2. Υποθέτουμε βεβαίως ότι υπάρχει φυσική πρόσβαση στον υπολογιστή, καθώς κι ότι ο boot manager είναι ο GRUB2. Παρόμοια εργαζόμαστε κι όταν αντί για openSUSE ο υπολογιστής τρέχει Ubuntu ή Fedora. Ένα ή δύο σημεία που χρειάζονται προσοχή τα επισημαίνουμε προς το τέλος του άρθρου.



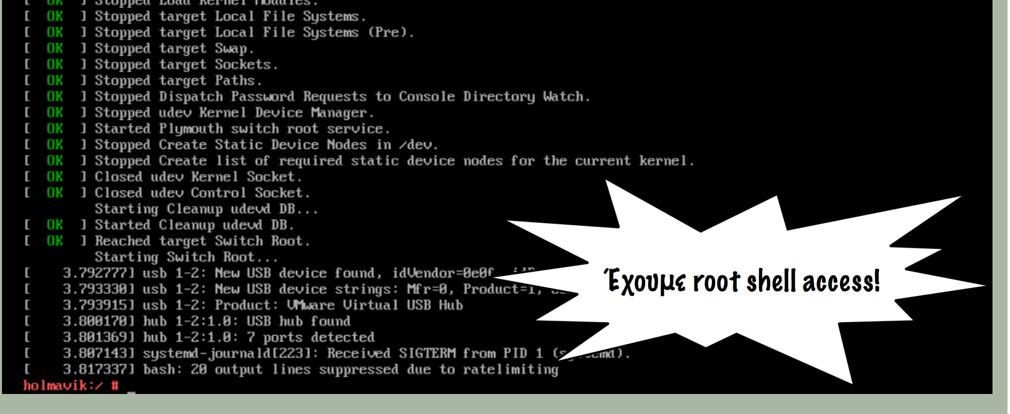
Βήμα 1. Ξεκινάμε ή επανεκκινούμε το μηχάνημα και μόλις εμφανιστεί η οθόνη του GRUB2 για την επιλογή boot entry, πριν τελειώσει το count down μετακινούμαστε με τα βελάκια του δρομέα πάνω από τη γραμμή που αντιστοιχεί στο φυσιολογικό φόρτωμα του λειτουργικού (συνήθως πρόκειται για την πρώτη επιλογή). Αντί για το πλήκτρο [Enter] πατάμε το [E] (από το Edit).



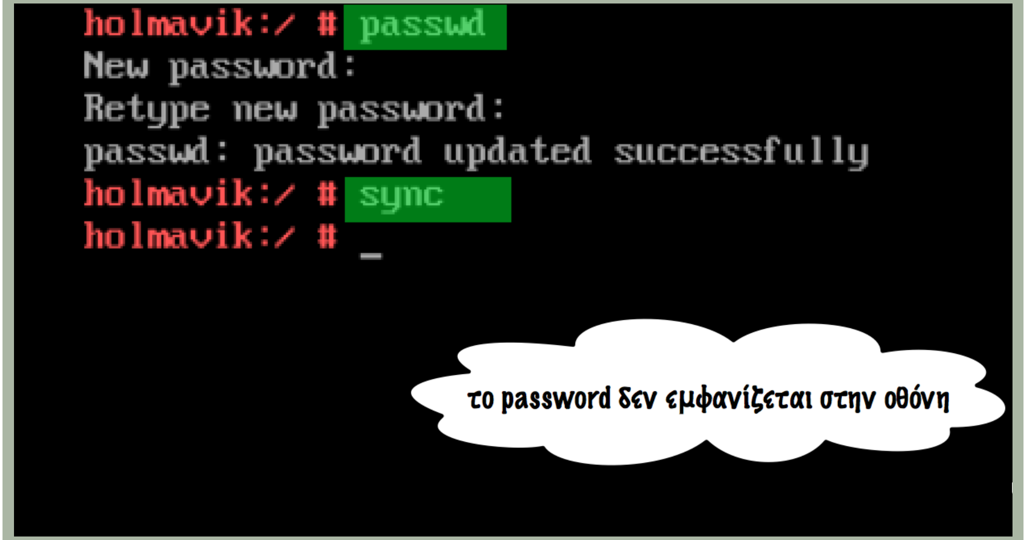
Βήμα 2. Βλέπουμε τώρα το τμήμα από το configuration του GRUB2, το οποίο αντιστοιχεί στο επιλεγμένο boot entry. Με το κάτω βελάκι μετακινούμαστε στο τέλος της οδηγίας που αρχίζει με "linux" (χωρίς τα εισαγωγικά). Πιθανότατα δεν θα χωρά σε μία μόνο γραμμή και θα εκτείνεται σε περισσότερες. Στο παράδειγμά μας φαίνεται να καταλαμβάνει τρεις γραμμές (εξαιτίας ενός και μόνο χαρακτήρα).



Βήμα 3. Στο τέλος της γραμμής αφήνουμε ένα κενό και πληκτρολογούμε "rw init=/bin/bash" (χωρίς τα εισαγωγικά). Βεβαιωνόμαστε ότι δεν έχουμε κάνει κάποιο λάθος πληκτρολόγησης και πατάμε το συνδυασμό πλήκτρων [CTRL+X]. Ξεκινά τότε το φόρτωμα της διανομής, αλλά αυτή τη φορά λαμβάνοντας υπόψη την τροποποιημένη οδηγία.



Βήμα 4. Ελάχιστα δευτερόλεπτα αργότερα η διαδικασία εκκίνησης θα έχει ολοκληρωθεί. Δεν θα είμαστε στο περιβάλλον γραφικών, ούτε σε κάποια text console όπου θα μας ζητείται σύνδεση σε λογαριασμό χρήστη. Αντίθετα, θα βρισκόμαστε σε ένα BASH shell και μάλιστα μέσα από το λογαριασμό του χρήστη root!



Βήμα 5. Για την αλλαγή του ξεχασμένου password χρησιμοποιούμε το εργαλείο passwd. Θα μας ζητηθεί να πληκτρολογήσουμε το νέο συνθηματικό – δύο φορές, ώστε να είμαστε βέβαιοι για το τι δώσαμε. Και λέμε να είμαστε βέβαιοι διότι, για λόγους ασφαλείας, καθώς πληκτρολογούμε το password οι χαρακτήρες δεν εμφανίζονται στην οθόνη. Αμέσως μετά γράφουμε sync και πατάμε το [Enter], προκειμένου να διασφαλίσουμε πως ό,τι είναι να γραφτεί στο δίσκο θα γραφτεί τώρα (και δεν θα παραμείνει στην cache). Μόλις ορίσαμε νέο password για τον χρήστη root – κι ας μην θυμόμαστε το παλιό! Για την επανεκκίνηση του συστήματος πληκτρολογούμε "/sbin/reboot -f" (φυσικά χωρίς τα εισαγωγικά).

Περίπτωση Ubuntu. Σε αντίθεση με το openSUSE και άλλες διανομές Linux, όταν στον υπολογιστή έχουμε εγκατεστημένο το Ubuntu τότε δεν βλέπουμε το μενού του GRUB2 κατά την (επαν)εκκίνηση του συστήματος. Για το πείσουμε να εμφανιστεί, (επαν)εκκινούμε κι αμέσως μετά τα μηνύματα POST κρατάμε το πλήκτρο [Shift] πατημένο μέχρι να το δούμε. Στη συνέχεια προχωράμε κι αλλάζουμε root password κατά τα γνωστά.

Περίπτωση Fedora. Αφού ορίσουμε το νέο password και πριν το sync (και την επανεκκίνηση), λόγω SELinux πληκτρολογούμε "touch /.autorelabel" (πάντα χωρίς τα εισαγωγικά). Κατά την εκκίνηση πιθανώς θα παρατηρήσετε ότι το σύστημα αργεί κάπως να σηκωθεί και να μας φέρει στην οθόνη σύνδεσης. Το γεγονός αυτό οφείλεται στο SELinux και συμβαίνει μόνο στην πρώτη επανεκκίνηση μετά την αλλαγή root password.

Skill: Beginner
Tags: ISO, USB, burning, Linux, macOS, Windows

Πώς γράφουμε αρχεία ISO σε USB sticks, από οποιοδήποτε λειτουργικό σύστημα

Οι νεοφερμένοι στον κόσμο του Linux συχνά ακούτε και διαβάζετε ότι πρέπει να κατεβάσετε το τάδε ISO image και μετά να το γράψετε σε CD, DVD ή USB stick. Για τέτοιες δουλειές παλιότερα χρησιμοποιούσαμε δισκάκια CD/DVD, σήμερα όμως είναι προτιμότερο να καταφεύγουμε σε USB sticks. Σε κάθε περίπτωση, η εγγραφή αρχείου ISO δεν σημαίνει ότι απλά το αντιγράφουμε στο νέο μέσο.

Τα αρχεία ISO μπορούμε να τα φανταζόμαστε ως ακριβή αντίγραφα αποθηκευτικών μέσων, τα οποία τις περισσότερες φορές είναι bootable. Ας υποθέσουμε για παράδειγμα ότι θέλουμε να εγκαταστήσουμε στον υπολογιστή μας το openSUSE Leap 42.2 (https://www.opensuse.org). Πρώτη μας δουλειά είναι να κατεβάσουμε το ISO image που "μέσα" του έχει τον installer του Leap, εκατοντάδες (ή μάλλον χιλιάδες) πακέτα εργαλείων κι εφαρμογών, καθώς κι ένα σωρό άλλα συνοδευτικά αρχεία. Το εν λόγω ISO image είναι bootable. Αυτό σημαίνει ότι αν το γράψουμε με τον *κατάλληλο* τρόπο σε δισκάκι DVD (δεν χωράει σε CD) ή σε USB stick (επαρκούς χωρητικότητας) και φροντίσουμε ώστε ο υπολογιστής μας να ξεκινήσει από το δισκάκι ή το στικάκι, τότε θα φορτώσει ο boot loader του ISO και θα έχουμε την ευκαιρία να ξεκινήσουμε τον installer του openSUSE, επομένως και να εγκαταστήσουμε το συγκεκριμένο λειτουργικό.

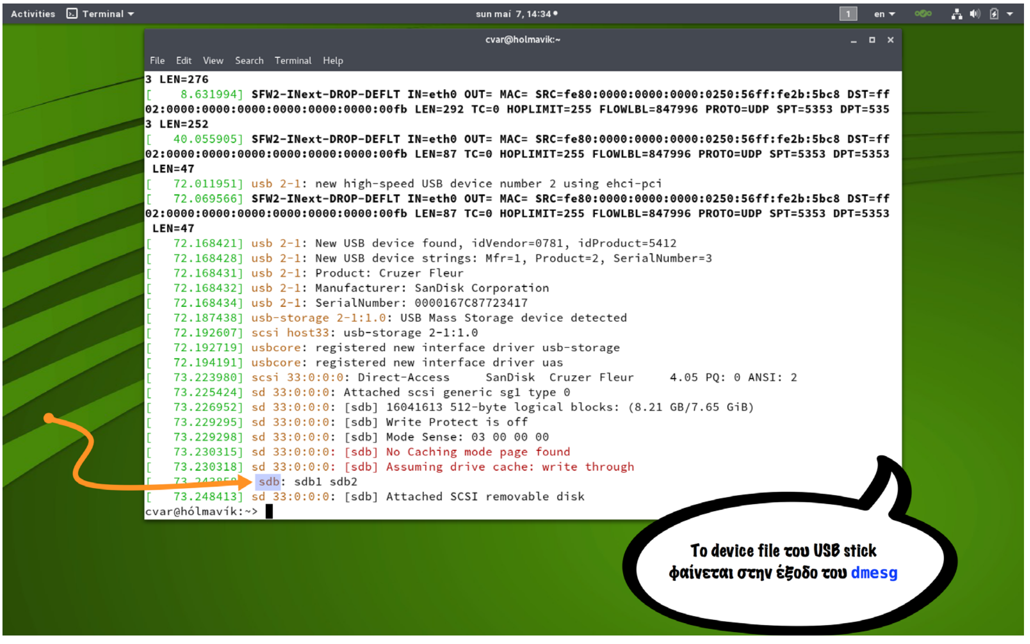
Το μυστικό εδώ είναι ότι τα ISO images δεν τα μεταφέρουμε σε CD/DVD/USB sticks, όπως θα μεταφέραμε ένα οποιοδήποτε άλλο αρχείο. Αντίθετα, για την εγγραφή του ISO image χρειαζόμαστε το κατάλληλο εργαλείο. Στη συνέχεια δείχνουμε πώς δουλεύουμε όταν είμαστε σε Linux, σε macOS ή σε Windows, προκειμένου να γράφουμε το ISO image του openSUSE Leap 42.2 σε USB stick.

Σημείωση. Αναφερόμαστε στο "μεγάλο" ISO image, χωρητικότητας 4,7GB, το οποίο περιλαμβάνει όλα τα απαιτούμενα πακέτα ώστε η εγκατάσταση να πραγματοποιείται χωρίς κατέβασμα πρόσθετων στοιχείων από το Internet (http://download.opensuse.org/distribution/leap/42.2/iso/openSUSE-Leap-42.2-DVD-x86_64.iso). Προφανώς, παρόμοια εργαζόμαστε αν αντί για το ISO του openSUSE έχουμε ένα μιας οποιασδήποτε άλλης διανομής Linux, μιας εκδοχής του BSD κ.ο.κ.

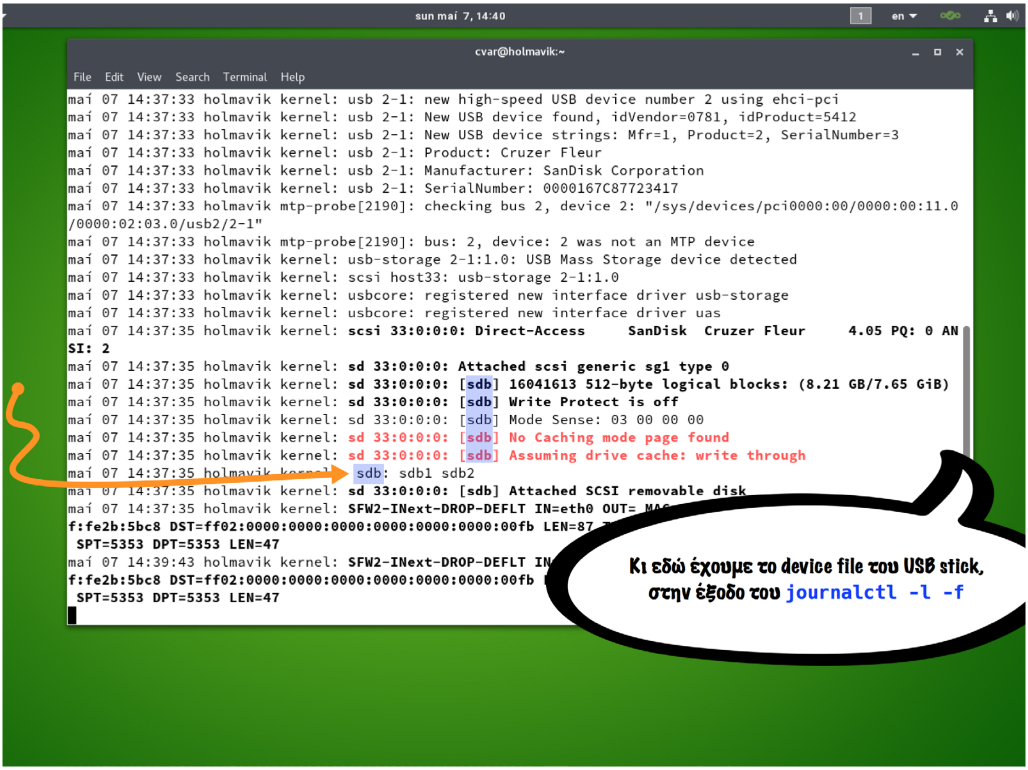
Προσοχή! Ασχέτως του λειτουργικού συστήματος από το οποίο εργαζόμαστε κι ασχέτως της μεθόδου που ακολουθούμε, η εγγραφή ISO image σε ένα οποιοδήποτε μέσο σημαίνει ότι τα δεδομένα που ενδεχομένως περιέχει το μέσο χάνονται αμετάκλητα. Αν λοιπόν στο USB stick σας βρίσκονται αρχεία που τα χρειαζόσαστε, φροντίστε τώρα για ένα καλό backup. Μετά το backup, ελέγξτε ξανά. Σοβαρά μιλάμε.

Εργασία από Linux

Πρώτη μας δουλειά είναι να βρούμε το device file που αντιστοιχεί στο USB stick. Αμέσως μετά γράφουμε το αρχείο ISO επί του USB καταφεύγοντας στο εργαλείο dd. Ένας τρόπος για να βρούμε το device file του USB είναι να συνδέσουμε το stick στον υπολογιστή, σε ένα τερματικό να τρέξουμε το εργαλείο dmesg, και στην έξοδό του να παρατηρήσουμε το ζητούμενο device file. Εναλλακτικά, σε διανομές Linux με το Systemd μπορούμε να βρούμε το ζητούμενο device file στην έξοδο του journalctl (https://deltahacker.gr/?p=16816).



Συνδέουμε το USB stick στον υπολογιστή μας και σε ένα τερματικό τρέχουμε το dmesg (δεν χρειάζονται δικαιώματα διαχειριστή). Στην έξοδο του εργαλείου υπάρχει και το device file του stick. Στο παράδειγμά μας είναι το sdb, επομένως το πλήρες path είναι το /dev/sdb.



Σε διανομές Linux που βασίζονται στο Systemd, σε ένα τερματικό μπορούμε να πληκτρολογήσουμε systemctl -l -f (με δικαιώματα διαχειριστή) κι αμέσως θ' αρχίσουμε να βλέπουμε ζωντανά τα logs του συστήματος. Συνδέοντας στον υπολογιστή το USB stick, στο τερματικό θα εμφανιστεί το device file του.

Αφού μάθουμε το device file του USB stick, γράφουμε πάνω του το ISO image με χρήση του εργαλείου dd. Πιο συγκεκριμένα, με δικαιώματα διαχειριστή συστήματος πληκτρολογούμε κάτι σαν

```
dd if=/home/cvar/Sóttar\ skrár/openSUSE-Leap-42.2-DVD-x86_64.iso of=/dev/sdb
bs=4M status=progress && sync
```

Αναλυτικότερα: Στην παράμετρο if δίνουμε την πλήρη διαδρομή του ISO image, στην παράμετρο of δίνουμε την πλήρη διαδρομή του device file του USB stick, ενώ με την παράμετρο bs ζητάμε η ανάγνωση και η εγγραφή δεδομένων να γίνεται σε τμήματα των 4 megabytes. Με αυτό το status=progress, εξάλλου, λέμε στο dd να μας δείχνει στο τερματικό την πρόοδο της διαδικασίας εγγραφής. Με την παράμετρο sync, τέλος, βεβαιωνόμαστε ότι δεν θα υπάρχουν δεδομένα στην cache που δεν έχουν ακόμη γραφτεί στο USB stick, οπότε μετά την εγγραφή του ISO αν θέλουμε θα αποσυνδέσουμε το στικάκι χωρίς καθυστέρηση.

```
cvar@hólmavík:~>
cvar@hólmavík:~> sudo dd if=/home/cvar/Sóttar\ skrár/openSUSE-Leap-42.2-DVD-x86_64.iso of=/dev/sdb bs=4M status=progress && sync
4378853376 bytes (4,4 GB, 4,1 GiB) copied, 506,143 s, 8,7 MB/s
1045+1 records in
1045+1 records out
4384096256 bytes (4,4 GB, 4,1 GiB) copied, 532,01 s, 8,2 MB/s
cvar@hólmavík:~>
```

Εγγραφή του ISO image (του openSUSE Leap 42.2) σε USB stick κατάλληλης χωρητικότητας, με τη βοήθεια του εργαλείου dd.

Εργασία από macOS

Στο macOS δουλεύουμε όπως περίπου και στο Linux, δηλαδή από ένα παράθυρο τερματικού και με τη βοήθεια του εργαλείου dd. Υπάρχουν όμως και κάποιες διαφορές, π.χ., στον τρόπο εντοπισμού του device file που αντιστοιχεί στο USB stick. Δείτε τα τρία screenshots που ακολουθούν, διαβάστε βεβαίως και τις αντίστοιχες περιγραφές.

```
mbpr15:~ cvar$
mbpr15:~ cvar$ diskutil list
/dev/disk0 (internal, physical):
   #:                       TYPE NAME                    SIZE       IDENTIFIER
   0:      GUID_partition_scheme                        *500.3 GB   disk0
   1:                        EFI EFI                     209.7 MB   disk0s1
   2:          Apple_CoreStorage Macintosh HD            499.4 GB   disk0s2
   3:                 Apple_Boot Recovery HD             650.0 MB   disk0s3

/dev/disk1 (internal, virtual):
   #:                       TYPE NAME                    SIZE       IDENTIFIER
   0:                  Apple_HFS MBPr15                 +499.1 GB   disk1
                                 Logical Volume on disk0s2
                                 BDA211BD-9E96-49C7-B4FA-76595AEAB9C8
                                 Unencrypted

/dev/disk2 (external, physical):
   #:                       TYPE NAME                    SIZE       IDENTIFIER
   0:     FDisk_partition_scheme                        *8.2 GB     disk2
   1:                 DOS_FAT_32 U                       8.2 GB     disk2s1

mbpr15:~ cvar$
```

*Συνδέουμε το USB stick στον υπολογιστή και σε ένα παράθυρο τερματικού πληκτρολογούμε diskutil list, ώστε να δούμε τα device files *όλων* των αποθηκευτικών μέσων που βλέπει το macOS. Στο παράδειγμά μας, το device file του stick είναι το /dev/disk2. Ένας τρόπος προκειμένου να είμαστε βέβαιοι πως κοιτάζουμε το σωστό device file, είναι να λαμβάνουμε υπόψη το μέγεθος του USB stick. Το δικό μας έχει μέγεθος 8GB οπότε, ναι, το device file που θέλουμε είναι το /dev/disk2.*

```
mbpr15:~ cvar$
mbpr15:~ cvar$ diskutil unmountDisk /dev/disk2
Unmount of all volumes on disk2 was successful
mbpr15:~ cvar$
```

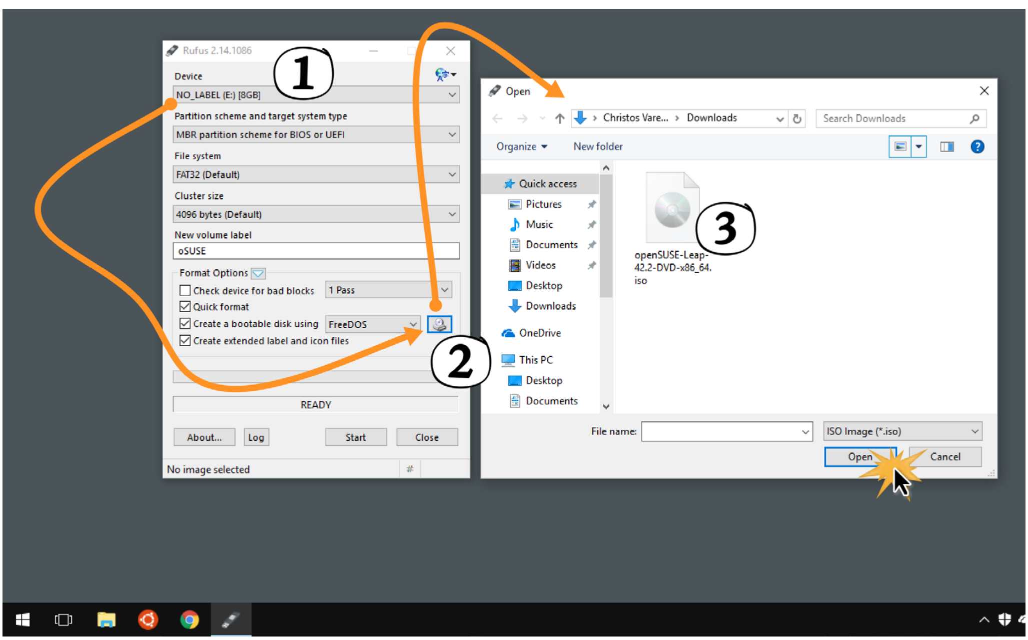
Πριν προχωρήσουμε στην εγγραφή του ISO αποπροσαρτούμε το USB stick, πληκτρολογώντας diskutil unmountDisk /dev/disk2. Βεβαίως, στη θέση του /dev/disk2 εσείς θα βάλετε το devife file για το δικό σας στικάκι.

```
mbpr15:~ cvar$
mbpr15:~ cvar$ sudo dd if=~/Downloads/openSUSE\ Leap\ 42.2\ DVD-x86_64.iso of=/dev/rdisk2 bs=4m
Password:
1045+1 records in
1045+1 records out
4384096256 bytes transferred in 494.012465 secs (8874465 bytes/sec)
mbpr15:~ cvar$
```

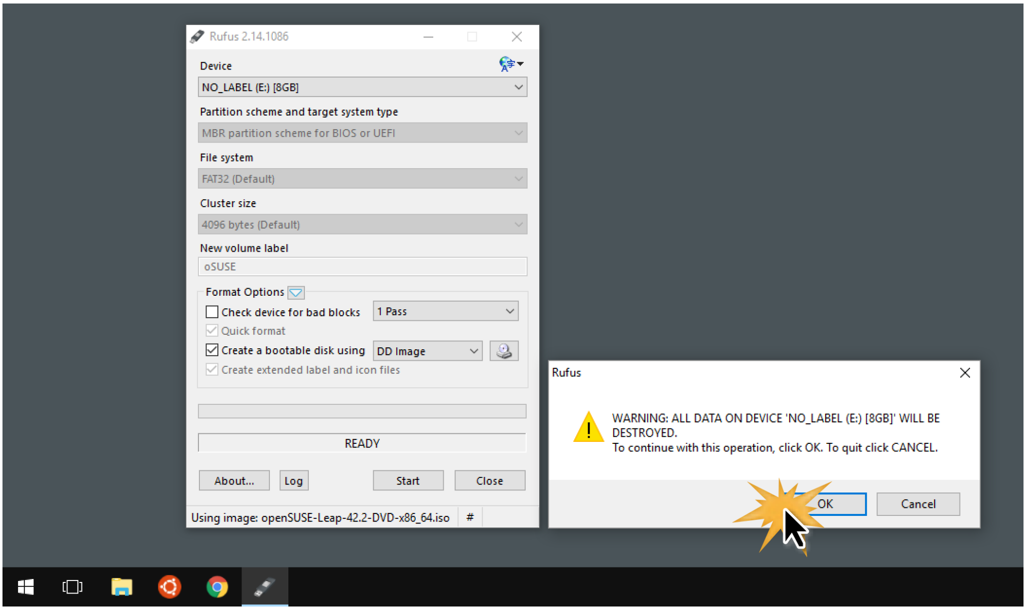
Και μετά την αποπροσάρτηση του USB stick ξεκινάμε την εγγραφή του ISO image, με τη βοήθεια του dd. Είναι φανερό ότι στην παράμετρο if δίνουμε το πλήρες path προς το αρχείο ISO, στην παράμετρο of δίνουμε το (πλήρες) όνομα του device file που αντιστοιχεί στο USB stick, ενώ με την παράμετρο bs ζητάμε η ανάγνωση και η εγγραφή δεδομένων να γίνεται σε τμήματα των 4 megabytes. Οι προσεκτικοί θα διαμαρτύρεστε ήδη: αντί για "disk2" έχουμε πληκτρολογήσει rdisk2. Αυτό το "r" προέρχεται από το "raw" και στην περίπτωσή μας σημαίνει ότι η εγγραφή επί του USB stick πραγματοποιείται ταχύτερα.

Εργασία από Windows

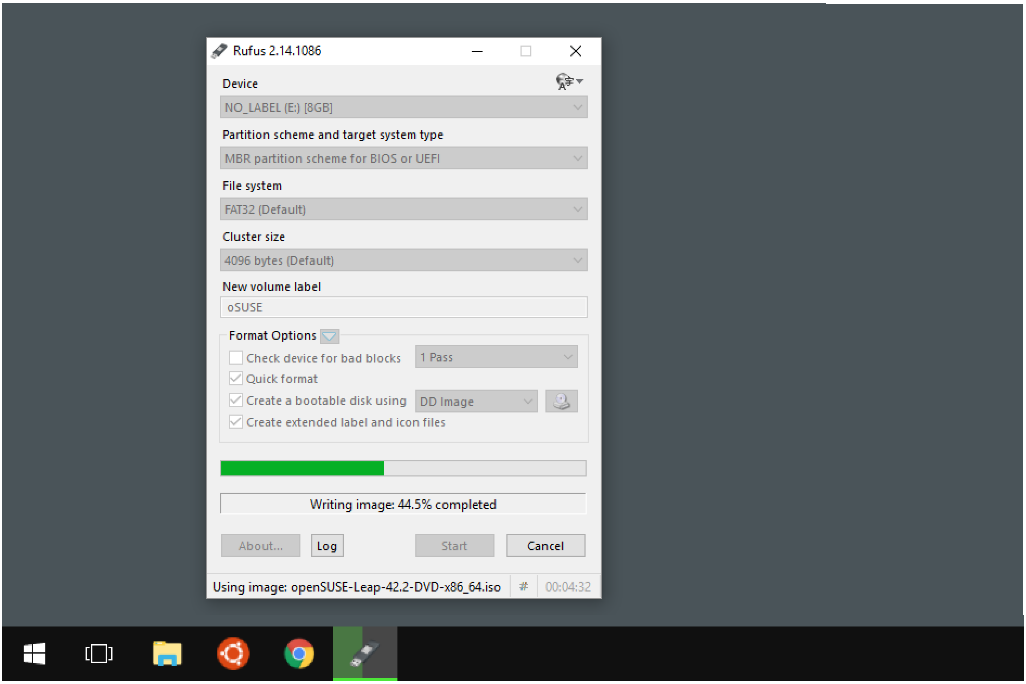
Ένας τρόπος για να γράφουμε ISO images σε USB sticks κάτω από Windows, είναι με τη βοήθεια της εφαρμογής Rufus (https://rufus.akeo.ie). Δείτε τα τέσσερα screenshots που ακολουθούν, διαβάστε και τις αντίστοιχες περιγραφές.



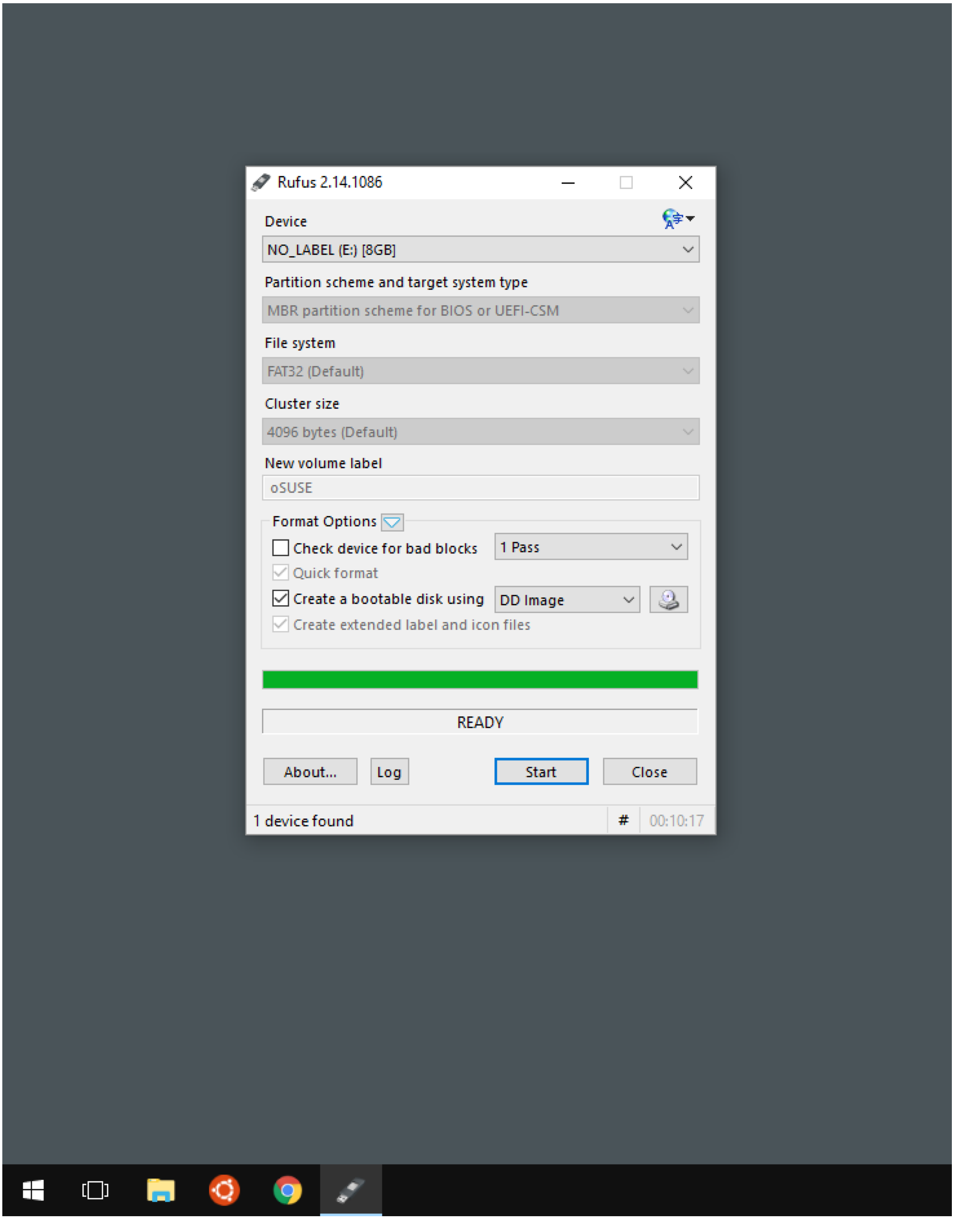
Τρέχουμε το Rufus και στη θυρίδα Device, στο βασικό παράθυρο της εφαρμογής, επιλέγουμε το drive letter που αντιστοιχεί στο USB stick (1). Κάνουμε ένα κλικ στο σχετικό εικονίδιο επιλογής αρχείων (2) κι αμέσως ανοίγει ένα παράθυρο του File Explorer των Windows. Απ' αυτό εντοπίζουμε κι επιλέγουμε το ISO image που θέλουμε να γράψουμε στο USB stick (3) και φυσικά πατάμε στο κουμπί Open.



Τα υπάρχοντα δεδομένα του USB stick πρόκειται να χαθούν! Γι' αυτό και το Rufus εμφανίζει παράθυρο με σχετική προειδοποίηση, καλώντας μας να επιβεβαιώσουμε την ενέργεια που πρόκειται να γίνει – ή βεβαίως να την ακυρώσουμε.



Η εγγραφή του ISO image επί του USB stick έχει ξεκινήσει κι εξελίσσεται ομαλά. Την πρόοδο της διαδικασίας τη βλέπουμε στη σχετική μπάρα, κάτω.



Η επιτυχής ολοκλήρωση της εγγραφής δεν συνοδεύεται από τυμπανοκρουσίες – αλλά ποιος νοιάζεται για τέτοια; Σημασία έχει ότι από το USB stick μπορείτε πλέον να ξεκινήστε την εγκατάσταση του άλλου σας αγαπημένου λειτουργικού.

Skill: Intermediate
Tags: AutoYaST, YaST, openSUSE

Αυτοματοποιημένες εγκαταστάσεις με το AutoYaST

Είστε υπεύθυνος για την εγκατάσταση διανομής Linux σε όλους τους υπολογιστές ενός τοπικού δικτύου. Δεχτείτε παρακαλούμε τα συγχαρητήριά μας – και καλό σας κουράγιο. Κάθε γνήσιο geek σίγουρα χαίρεται όταν του δίνεται η ευκαιρία να χαρίσει ζωή σε μια μηχανή, ξεκινώντας με την εγκατάσταση του OS. Τι γίνεται όμως όταν αντί για έναν ή δύο υπολογιστές έχουμε πέντε, δέκα ή ακόμη και περισσότερους; Ποιος μπορεί να αντέξει τόση χαρά, ειδικά όταν υπάρχει και deadline;

Το πρόβλημα που μόλις περιγράψαμε έχει περισσότερες από μία λύσεις. Ίσως, π.χ., υπάρχει πρόσβαση σε PXE boot server, οπότε οι υπολογιστές του δικτύου ξεκινούν απ' αυτόν φορτώνοντας το κατάλληλο image και στη συνέχεια πραγματοποιείται η εγκατάσταση του λειτουργικού. Μια άλλη προσέγγιση είναι να ολοκληρωθεί η εγκατάσταση σε έναν μόνον υπολογιστή και μετά, με κάποιον τρόπο, τα περιεχόμενα του δίσκου να αντιγραφούν, bit προς bit, στους δίσκους των άλλων υπολογιστών. Βεβαίως, η αντιγραφή θα χρειαστεί να γίνει με τέτοιο τρόπο, ώστε μετά το πέρας της οι άλλοι υπολογιστές να είναι bootable. Σκεφτείτε επίσης ότι τα μηχανήματα τα οποία πρόκειται να δεχτούν το νέο λειτουργικό θα στερούνται πρόσβασης στο δίκτυο. Θα πρέπει λοιπόν είτε να φορτώσουν πρώτα κάποιο μίνι-λειτουργικό με το κατάλληλο λογισμικό (είπε κανείς "κλοουνζίλα"; (http://clonezilla.org)), είτε να έχουμε δίσκους που μεταφέρονται και συνδέονται σε εκείνον με την έτοιμη εγκατάσταση (αυτή τη φορά είμαστε 100% βέβαιοι ότι κάποιος είπε "ντι-ντι" (https://linux.die.net/man/1/dd)).

Στο παρόν άρθρο παρουσιάζουμε μια εντελώς διαφορετική, εξαιρετικά ευέλικτη λύση, η οποία ούτε την παρουσία PXE boot server προϋποθέτει, ούτε περίτεχνες και χρονοβόρες αντιγραφές χρειάζεται. Μόνος περιορισμός είναι ότι αφορά σε εγκαταστάσεις openSUSE (https://www.opensuse.org) (ή SUSE Linux Enterprise (https://www.suse.com/products/server)). Από την άλλη, βέβαια, όταν αρχίζουμε να σκεφτόμαστε όλα –ή έστω μερικά από– τα μηχανήματα ενός τοπικού δικτύου, δύσκολα μπορούμε να φανταστούμε ότι __δεν__ θα τρέχουν openSUSE :P

Στο προκείμενο, μιλάμε για το AutoYaST: ένα πανίσχυρο σύστημα αυτόματης εγκατάστασης του openSUSE. Αναλυτικότερα, με κάποιον τρόπο που θα δούμε σε λίγο δημιουργούμε ένα AutoYaST profile. Αυτό δεν είναι τίποτε περισσότερο από ένα αρχείο XML με λεπτομερείς πληροφορίες εγκατάστασης και ρύθμισης. Από τη στιγμή που έχουμε το AutoYaST profile μας, προχωράμε κανονικά με την εγκατάσταση του openSUSE σε ένα οποιοδήποτε μηχάνημα. Μόνο που στις παραμέτρους που περνάμε στον πυρήνα, επιλέγοντας το κατάλληλο entry στο μενού του GRUB, υποδεικνύουμε τη θέση του XML. Μετά η εγκατάσταση του openSUSE ξεκινά κι ολοκληρώνεται αυτόματα – χωρίς επίβλεψη ή επεμβάσεις.

Για άλλη μια φορά, ο καλύτερος τρόπος προκειμένου να εκτιμήσετε το AutoYaST είναι να πειραματιστείτε, σε φυσικό ή σε εικονικό εργαστήριο. Στη συνέχεια δείχνουμε:

- πώς φτιάχνουμε ένα AutoYaST profile αυτόματα και γρήγορα, ξεκινώντας από μια υπάρχουσα εγκατάσταση του openSUSE
- πώς τροφοδοτούμε, δικτυακά, το profile στον installer του openSUSE
- τι κάνουμε στις περιπτώσεις που το hardware ενός υπολογιστή διαφέρει από το hardware που περιγράφεται στο εκάστοτε AutoYaST profile

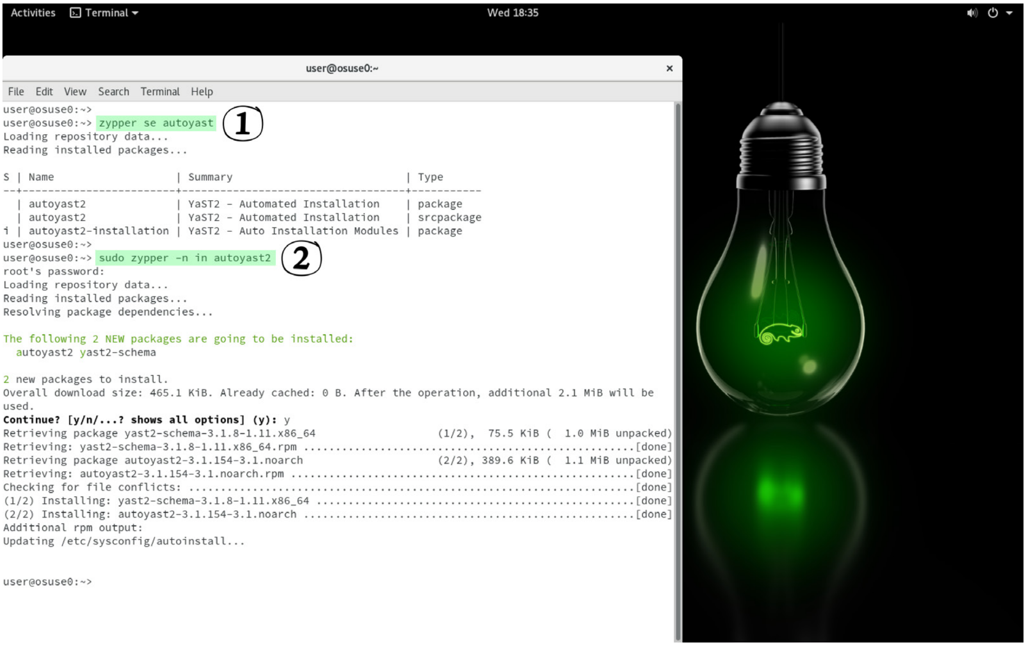
Δείτε τα screenshots που ακολουθούν, διαβάστε βεβαίως και το συνοδευτικό κείμενο.

Βήμα 1 | δημιουργία AutoYaST profile

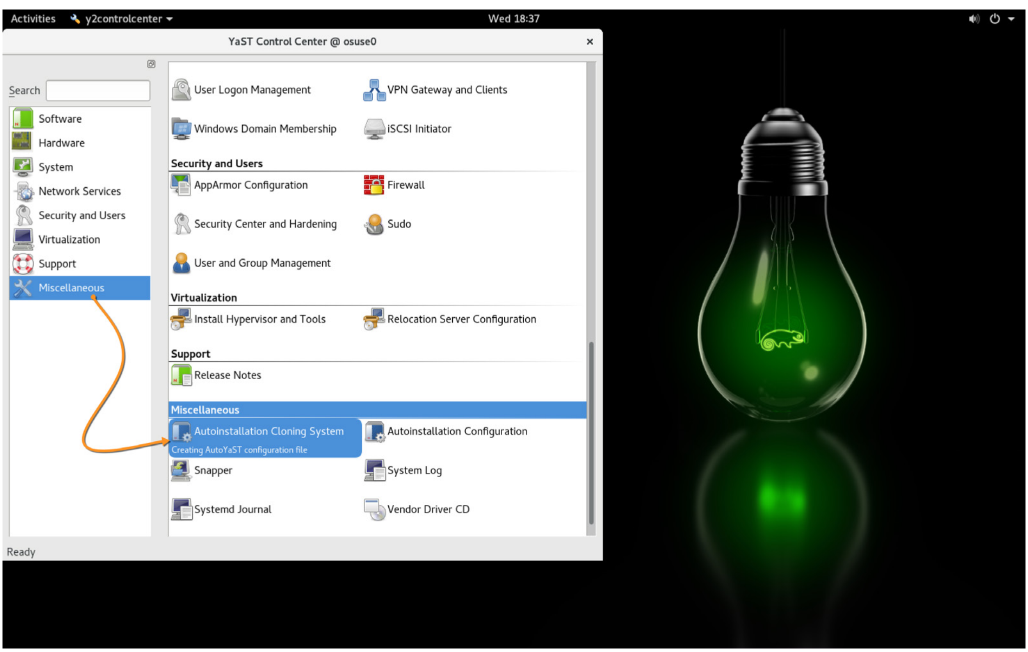
Δουλεύουμε στο osuse0.colder.is, έναν υπολογιστή με το openSUSE Leap ήδη εγκατεστημένο. Το σύστημα είναι προσβάσιμο από το τοπικό δίκτυο, οπότε οι άλλοι υπολογιστές, στους οποίους θα γίνουν αυτοματοποιημένες εγκαταστάσεις, θα είναι σε θέση να διαβάσουν το AutoYaST profile δικτυακά, χωρίς δηλαδή να απαιτείται η μεταφορά/περιφορά του (π.χ., με κάποιο USB stick). Περισσότερα επ' αυτού σε λίγο.

Φορτώνουμε λοιπόν το openSUSE Leap και με το zypper φροντίζουμε για την παρουσία του πακέτου autoyast2. Αυτό περιλαμβάνει το module του YaST για τη δημιουργία και γενικά για τη διαχείριση AutoYaST profiles.

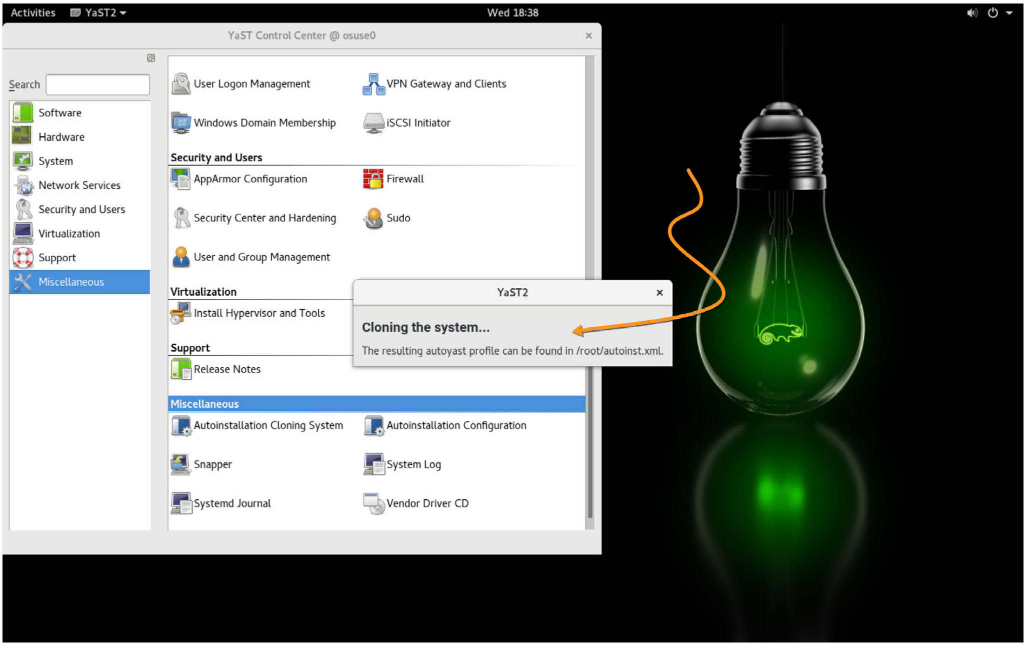
Το module το ξεκινάμε φορτώνοντας το YaST Control Center και μεταβαίνοντας στην κατηγορία Miscellaneous (βλ. αριστερό, κάθετο πλαίσιο). Εκεί υπάρχουν δύο entries σχετικά με το AutoYaST. Αυτό που μας ενδιαφέρει είναι το Autoinstallation Cloning System. Με κλικ πάνω του ξεκινά η διαδικασία δημιουργίας ενός AutoYaST profile, το οποίο αντικατοπτρίζει __επακριβώς__ τις επιλογές που κάναμε κατά την εγκατάσταση του συστήματος. Αναλυτικότερα, αναφερόμαστε σε επιλογές περί filesystems, λογαριασμών χρηστών, δικτύωσης, bootloader κ.λπ. Επιπλέον, αν μετά την εγκατάσταση κάναμε πρόσθετες αλλαγές στο σύστημα, όπως, π.χ., προσθήκη νέων λογαριασμών χρηστών, οι σχετικές πληροφορίες θα συμπεριληφθούν στο υπό δημιουργία profile.



Αναζητούμε κάποιο πακέτο που ονομάζεται "autoyast" ή κάπως έτσι (1). Το εντοπίζουμε, ονομάζεται "autoyast2", και το εγκαθιστούμε αμέσως (2).



Στο YaST Control Center πηγαίνουμε στην κατηγορία Miscallaneous και κάνουμε ένα κλικ στο Autoinstallation Cloning System. Σε πολύ λίγο θα έχουμε ένα AutoYaST profile που θα αντικατοπτρίζει την παρούσα εγκατάσταση.



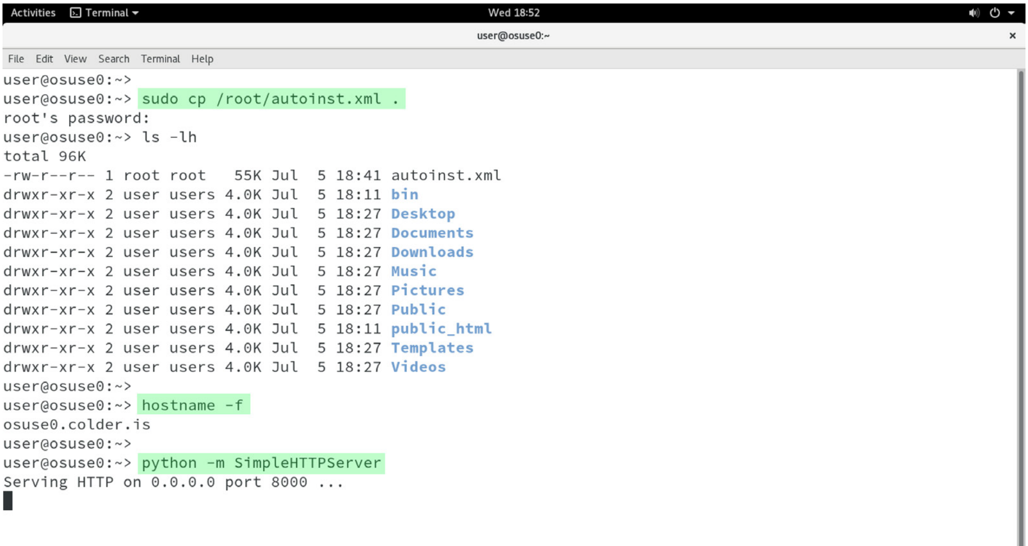
Το μήνυμα 'Cloning the system...' μοιάζει παραπλανητικό, αφού δεν λαμβάνει χώρα κάποια κλωνοποίηση του συστήματος, π.χ., με τη μορφή αντιγραφής. Δημιουργείται όμως ένα AutoYaST profile, το οποίο αν χρησιμοποιήσουμε κατά την εγκατάσταση του openSUSE σε άλλο μηχάνημα τότε θα καταλήξουμε με ένα σύστημα εντελώς παρόμοιο με αυτό που τώρα έχουμε.

Το AutoYaST profile δημιουργείται αυτόματα κι αποθηκεύεται στο αρχείο autoinst.xml, εντός του καταλόγου /root. Ίσως θέλουμε να το μεταφέρουμε σε κάποιον περισσότερο βολικό κατάλογο, ίσως κι όχι.

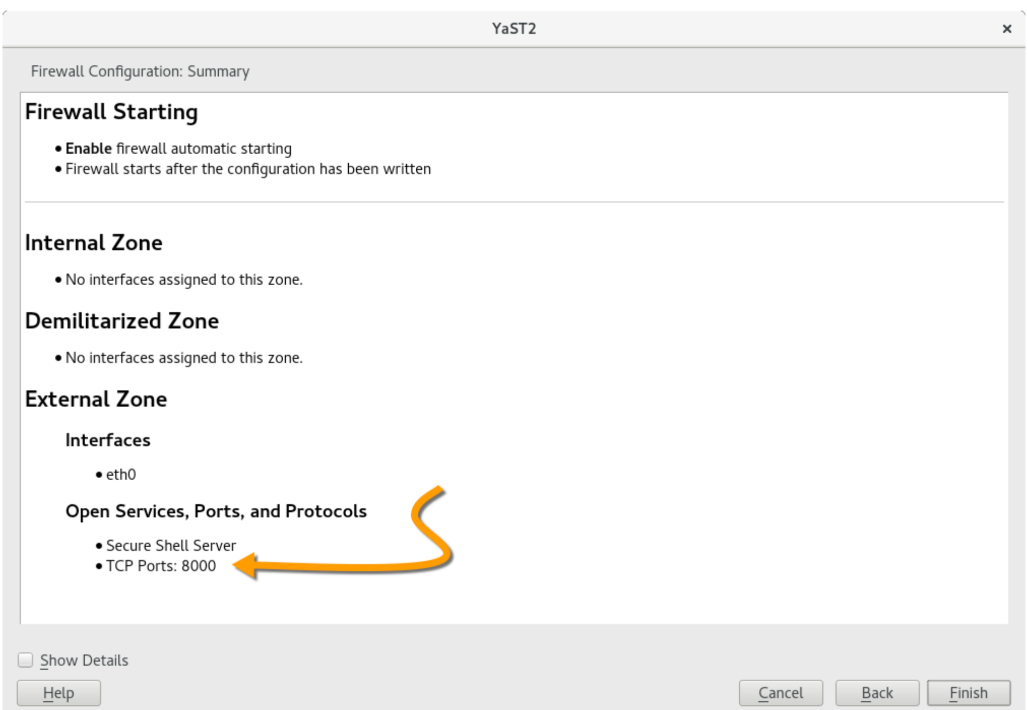
Το θέμα μας τώρα είναι ότι χρειάζεται να καταστήσουμε το autoinst.xml διαθέσιμο σε άλλους υπολογιστές του τοπικού δικτύου. Μπορούμε να καταφύγουμε στον Apache, στον nginx ή σε οποιονδήποτε άλλο web server. Ίσως όμως να μην έχουμε έναν ολόκληρο διακομιστή ιστοσελίδων διαθέσιμο – και για να λέμε τα πράγματα με τ' όνομά τους μάλλον θα ήταν υπερβολικό να επιστρατεύσουμε κάποιον μόνο και μόνο για το ταπεινό autoinst.xml. Ευτυχώς που είναι προεγκατεστημένη η Python, η οποία διαθέτει ένα module που λειτουργεί ως web server. Από ένα τερματικό, λοιπόν, μεταβαίνουμε στον κατάλογο του autoinst.xml και πληκτρολογούμε

```
python -m SimpleHTTPServer
```

Τότε, όλα τα περιεχόμενα του καταλόγου θα είναι διαθέσιμα μέσω HTTP και συγκεκριμένα από τη διεύθυνση http://suse0.colder.is:8000 (εξ ορισμού, ο SimpleHTTPServer ακούει για αιτήσεις πελατών από το port 8000/TCP). Φυσικά, αν δεν υπάρχει FQDN (στο παράδειγμά μας είναι το suse0.colder.is) τότε στη θέση του θα είναι αρκετό να βάλουμε τη διεύθυνση IP του μηχανήματος (192.168.193.243, πάντα για την περίπτωσή μας).



Η χρήση ενός κανονικού, full featured διακομιστή ιστοσελίδων όπως είναι ο Apache ή ο nginx, μάλλον αποτελεί υπερβολή για το σερβίρισμα του autoinst.xml. Γι' αυτό κι αντιγράφουμε το αρχείο XML στον προσωπικό κατάλογο του χρήστη μας και φορτώνουμε το SimpleHTTPServer module της Python.



Το module ονόματι SimpleHTTPServer της Python εξ ορισμού χρησιμοποιεί το port 8000/TCP. Αν στο σύστημά μας το firewall είναι ενεργοποιημένο, φροντίζουμε ώστε να επιτρέπονται οι εισερχόμενες συνδέσεις στο προαναφερθέν port.

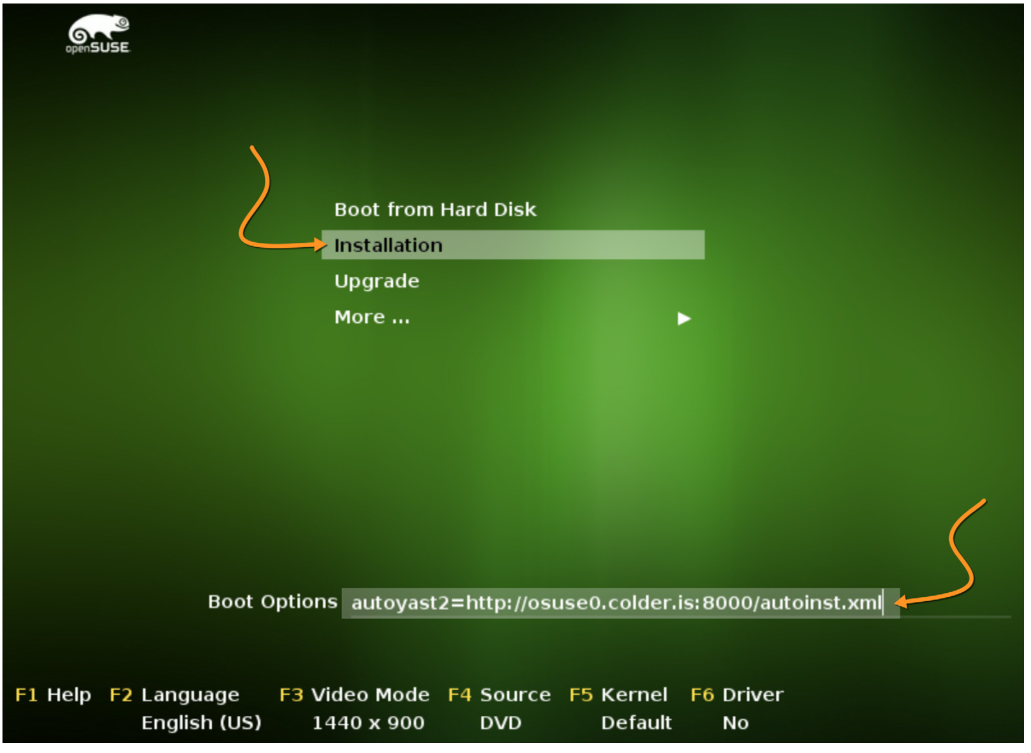
Σημείωση. Αν έχουμε το firewall ενεργοποιημένο, στο σημείο αυτό οφείλουμε να φροντίσουμε ώστε οι συνδέσεις στο port 8000/TCP να επιτρέπονται από hosts του λεγόμενου External Zone – μ' άλλα λόγια από μηχανήματα του τοπικού δικτύου. Η ρύθμιση του firewall γίνεται πανεύκολα με τη βοήθεια του YaST και συγκεκριμένα χάρη στο module ονόματι firewall.

Βήμα 2 | αυτόματη εγκατάσταση με χρήση AutoYaST profile

Πηγαίνουμε τώρα σε έναν άλλον υπολογιστή και ξεκινάμε την εγκατάσταση του openSUSE, από DVD ή USB stick. Στην πρώτη οθόνη του installer, με τα βελάκια του δρομέα μετακινούμαστε πάνω από το entry με όνομα Installation αλλά __δεν__ πατάμε το [Enter]. Πρώτα, στη θυρίδα Boot Options πληκτρολογούμε

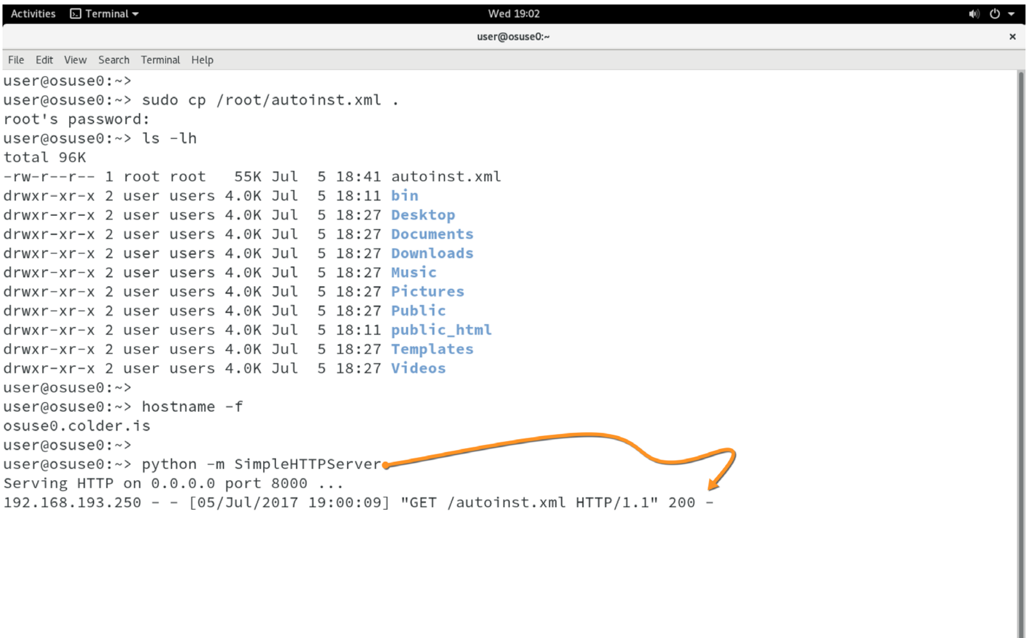
```
autoyast2=http://osuse0.colder.is:8000/autoinst.xml
```

Φυσικά, στη θέση του osuse0.colder.is εσείς θα βάλετε το κατάλληλο FQDN ή την κατάλληλη διεύθυνση IP. Επίσης, αν ο απομακρυσμένος web server χρησιμοποιεί το τυπικό port (80/TCP), τότε θα παραλείψετε αυτό το ":8000".



Πριν ακόμη φορτώσουμε τον installer για την εγκατάσταση του openSUSE Leap σε κάποιον άλλον υπολογιστή, με την εικονιζόμενη οδηγία φροντίζουμε ώστε να διαβαστεί το AutoYaST profile που δημιουργήσαμε προηγουμένως. Κατ' αυτόν τον τρόπο η νέα εγκατάσταση θα πραγματοποιηθεί αυτόματα και χωρίς καμία παρέμβαση από μέρους μας.

Αφού βεβαιωθούμε ότι δεν έχουμε κάνει κάποιο λάθος πληκτρολόγησης, πατάμε το [Enter] και η διαδικασία της αυτόματης εγκατάστασης ξεκινά. Ίσως δεν προλάβετε να δείτε το μήνυμα που φανερώνει ότι το αρχείο autoinst.xml διαβάστηκε. Θα το καταλάβετε όμως αν ρίξετε μια ματιά στο τερματικό απ' όπου ξεκινήσατε το SimpleHTTPServer module της Python – ή στο log file του web server που χρησιμοποιείτε, τέλος πάντων.



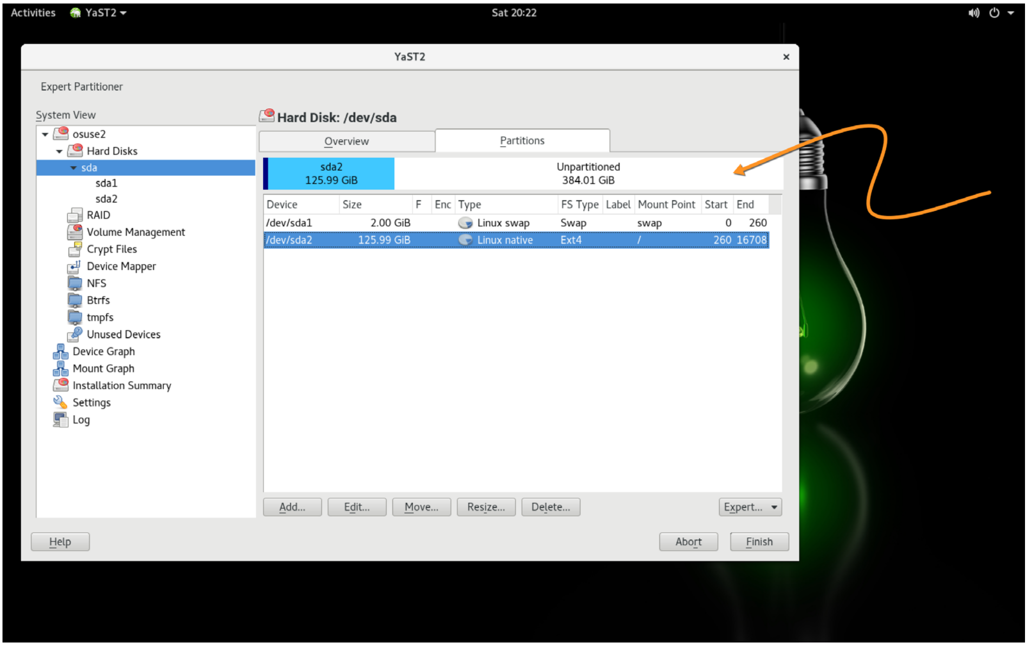
Ίσως δεν προλάβουμε να δούμε κάτι σχετικό στα μηνύματα που εμφανίζονται στην οθόνη του νέου συστήματος, παρατηρώντας όμως το τερματικό από το οποίο φορτώσαμε το SimpleHTTPServer module της Python αμέσως διαπιστώνουμε πως το AutoYaST profile διαβάστηκε από τον installer.

Καθ' όλη τη διάρκεια της εγκατάστασης δεν θα χρειαστεί να κάνετε κάτι, όλα θα γίνουν αυτοματοποιημένα. Κάποια στιγμή ο installer θα επανεκκινήσει το σύστημα και θα ξεκινήσει μια διαδικασία αναγνώρισης και ρύθμισης του hardware. Θα ακολουθήσει άλλο ένα reboot και θα βρεθούμε μπροστά από ένα πλήρως ρυθμισμένο λειτουργικό, παρόμοιο με εκείνο στο osuse0.colder.is.

Βήμα 3 | προσαρμογή στο hardware του εκάστοτε host

Ένα ή περισσότερα από τα PCs στα οποία εγκαθιστάτε το openSUSE σας αυτόματα, με το AutoYaST, ίσως έχουν διαφορετικά χαρακτηριστικά από το μηχάνημα στο οποίο δημιουργήσατε το AutoYaST profile. Σε τέτοιες περιπτώσεις, μετά την πρώτη εκκίνηση του λειτουργικού στο νέο PC, ίσως χρειαστεί να κάνετε μία ή δύο ρυθμίσεις. Σκεφτείτε, για παράδειγμα, ότι το αρχικό μηχάνημα είχε έναν μόνο δίσκο SSD, χωρητικότητας 128GB. Επιλέξατε να δημιουργήσετε ένα swap partition μεγέθους 2GB, ενώ όλο τον υπόλοιπο χώρο τον δώσατε στο root partition και, παρεμπιπτό-

ντως, το διαμορφώσατε κατά Ext4. Τώρα, ένα από τα μηχανήματα στα οποία εγκαθιστάτε το openSUSE αυτόματα, έχει δίσκο SSD χωρητικότητας 512GB. Μετά το πέρας της διαδικασίας εγκατάστασης θα διαπιστώσετε ότι ο δίσκος έχει: α) ένα διαμέρισμα swap μεγέθους 2GB, β) ένα root partition μεγέθους 126 (περίπου) GB, καθώς και γ) ελεύθερο χώρο 384GB που δεν έχει κατανεμηθεί σε καμία κατάτμηση. Είναι κρίμα να μένει όλος αυτός ο χώρος ανεκμετάλλευτος. Ευτυχώς, χάρη στο YaST –και συγκεκριμένα χάρη στο module ονόματι disk– είναι πολύ εύκολο να δημιουργήσετε μία ή περισσότερες νέες κατατμήσεις, τις οποίες και θα διαμορφώσετε κατά το filesystem της προτίμησής σας. Εναλλακτικά, κι επειδή το Ext4 filesystem το επιτρέπει, έχετε τη δυνατότητα να μεγεθύνετε το root partition __μη καταστροφικά__, ώστε να καταλαμβάνει περισσότερο χώρο ή ακόμη και όλον τον διαθέσιμο ελεύθερο χώρο.



Κατά περιπτώσεις, η αυτοματοποιημένη εγκατάσταση θα ολοκληρώνεται επιτυχώς αλλά θα χρειάζονται και κάποιες επεμβάσεις από μέρους μας. Ίσως, π.χ., το νέο σύστημα να έχει μεγαλύτερο δίσκο από το δίσκο του υπολογιστή στον οποίο φτιάξαμε το AutoYaST profile, οπότε τώρα έχουμε αποθηκευτικό χώρο που δεν έχει κατανεμηθεί. Χάρη στο module ονόματι disk του YaST, αυτή η κατάσταση διευθετείται πανεύκολα.

Χαρείτε το νέο σας τοπικό δίκτυο με openSUSE boxes, το οποίο καταφέρατε και στήσατε σε χρόνο ρεκόρ. Εκτός από εσάς, να είστε βέβαιοι ότι θα το χαρούν και οι χρήστες του.

deltahacker.gr